FICS Research

The Florida Institute *for* Cybersecurity Research

VOLUME II

GAINESVILLE, FL

352-294-3945

FICS.INSTITUTE.UFL.EDU

TABLE OF CONTENTS

ABOUT FICS RESEARCH

The Florida Institute for Cybersecurity (FICS) Research was established with the mission to become the nation's premier multidisciplinary research institute, seeking the advancement of cyber security as a basis for long-term partnership and collaboration among industry, academe, and government. FICS Research's objective is to directly support the research needs of industry and government partners in a cost-effective manner with pooled, leveraged resources and maximized synergy, as well as to enhance the educational experience for a diverse set of top-quality graduate and undergraduate students. FICS Research will work towards advancing knowledge and technologies in this emerging field, as well as ensure the commercial relevance of the research, by establishing spin off companies via rapid and effective technology transfer.

FICS Research is unique. It is arguably the only institute in the country that provides exceptional expertise in all aspects of cybersecurity and assurance, including hardware, network, mobile, big data, internet of things (IoT), applied crypto, social sciences, law, and more.

DIRECTOR

Mark Tehranipoor
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
ECE Department
University of Florida

ASSOCIATE DIRECTOR

Kevin Butler
Arnold and Lisa Goldberg Rising Star Associate Professor in Computer Science
Associate Professor
CISE Department
University of Florida

TECHNICAL AREAS

TA1: IoT Security

TA2: Biometrics

TA3: Hardware Security

TA4: Software Assurance / Security

TA5: Network Security

TA6: Applied Crypto / Theory

TA7: Usable Security

TA8: Privacy and Anonymity

TA9: Machine Learning for Cyber Defense

TA10: System Security

- TA10.1: Automotive Security
- TA10.2: Financial Security
- TA10.3: Cyber Physical Systems Security
- TA10.4: Bio-medical Systems Security

Research

PROJECT TITLES

01. Building a Private Bitcoin Payment Network using Off-chain Links

02. Drone ITS: Drone-aided Platform for Enabling Next Generation Intelligent Transport Systems

03. Efficient Public-Key Management for Smart Meter Communications

04. Lightweight Symmetric Key Management for Low-bandwidth Legacy Environments in Smart Grid

05. Mitigating Attacks towards Networked Cyber-physical Systems

06. SDN and NFV-based Moving Target Defense for Distributed Denial of Service Attacks

07. Vehicular Forensics Via Permissioned Blockchain

08. Automated Reverse Engineering of Integrated Circuits

09. Non-destructive Bond Pull and Ball Shear Tests for Electronics Quality Assurance and Counterfeit Detection through 3D X-ray Tomography and Finite Element Modeling

10. Trojan Scanner: Detecting Hardware Trojans with Rapid SEM Imaging combined with Image Processing and Machine Learning

11. Towards Provably Privacy-Preserving Data Analysis with Privacy Filters

12. Understanding Machine Learning Leaks: Causes and Defenses

13. Attention Based Secure Smart Image Sensor design for High-speed Real-Time secure vision applications.

14. Design of Secured MPSoC

15. Security in FPGA Accelerated Cloud and Datacenters

16. Towards a Practical and Secure FPGA-Based Digital Wallet

17. Intel SGX-aided Solutions: FORTIS

18. One-Time Programs

19. Privacy-Preserving Multiparty Computation

20. Vetting Embedded Firmware

21. AMS Circuit Obfuscation

22. Automated Security Property Mapping for Legacy Designs

23. Development of a Static Security Property Database
24. FPGA Bitstream Reverse Engineering-Based Device Upgrade
25. FPGA Trojan Detection using Static Design Analysis
26. Hardware Obfuscation Using HLS
27. Identifying Vulnerabilities Introduced by High-level Synthesis
28. Information Flow Tracking Based Software Vulnerabilities Detection
29. Metric-driven Security Property Verification
30. Security Verification of AI Systems
31. Security Verification using Formal Methods
32. SeRFI: Secure Remote FPGA Initialization in an Untrusted Environment
33. Security-preserving Post-silicon Validation and Debug
34. Aging-resistant FPGA RO PUF
35. Attacks and Countermeasures for Semiconductor IP Protection
36. Automated Counterfeit IC Defect Detection
37. Automated Non-Destructive PCB Reverse Engineering from X-Ray Computed Tomography
38. BLOcKeR: A Biometric Locking Paradigm for IoT and the Connected Person
39. Cardiovascular Biometric Authentication, Key Generation, and Presentation Attacks
40. Circuit Edit Enabled Trusted Fabrication for Low Volume Products
41. Covert Gates: Protecting Integrated Circuits from Reverse Engineering with Undetectable Camouflaging
42. Developing Low Cost Electrical Test Methods for Counterfeit FPGA Detection
43. EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection on Remarked and Cloned ICs
44. EMFORCED: EM-based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification
45. FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Today’s Complex Supply Chain
46. Hierarchical Bloom Filter (HBF) Framework for Security, Space-efficiency, and Rapid Query Handling in Biometric Systems

47. Intrinsic Memory-based Solutions Against Counterfeit ICs
48. Metrics and Benchmarking for Logic Locking and Hardware Obfuscation
49. Nanopyramids - Optical Scramblers for Protecting Against Backside Probing Attacks
50. Obfuscation-based PCB Anti-Reverse Engineering
51. PCB Tamper Detection
52. A provable-security Treatment of Counterfeiting Problems in Electronics Supply Chain
53. RASC: Enabling Remote Access to Side-Channels for Mission Critical Systems
54. Recycled/Remarked Detection of Analog/Mixed-Signal ICs via LDO
55. EM Side-Channel Based Hardware Security Analysis
56. Formal Security Validation on RTL Designs
57. Hardware Supported Virtual Machine Security Analysis in Cloud Environment
58. IoT Security Vulnerability Database Development
59. Logic Obfuscation for IP Protection
60. DeepSecurity
61. Beomsoo: High Precision Analog Mixed-Signal Circuitry for Counterfeit Detection and Securing Supply Chain
62. Cost-effective, Scalable, Portable All Digital Approach for Protection Against IC Recycling and Mitigation of Aging Effects
63. A Fully-Digital, Unclonable Security Protocol for Use in Analog/Mixed-Signal Systems
64. High Precision Analog Mixed-Signal Circuitry for Counterfeit Detection and Securing Supply Chain
65. PCB Assurance & Sensitivity Analysis
66. IC Trojan Insertion and Detection
67. Leveraging Passive Components in Silicon to Improve Security Merits
68. Intellectual Property (IP) Trust Validation using Formal Methods
69. System-on-Chip Security Validation using Side-Channel Analysis
70. Secure Network-on-Chip Architecture
71. Post-Silicon Validation and Debug

72. System-on-Chip Validation and Verification
73. Age-Targeted Automated Security Cueing Against Web-Based Social Engineering Attacks
74. Blind Spots - Building Developer Centric Security through Crowdsourcing
75. Collaborative: Developer Crowdsourcing: Capturing, Understanding, and Addressing Security-related Blind Spots in APIs
76. Fine-grained Analysis on Software Senility Towards System Unpredictabilities Attacks
77. FIRMA: Personalized, Cross-layered Continuous Authentication
78. Focused Security Behavior Nudging via Subliminal Stimuli
79. Machine Learning for Cyber Defense
80. RanStop: A Hardware-assisted Runtime Crypto-Ransomware Detection Technique
81. Security Estimation
82. Censorship Evasion
83. Hedged Cryptography: Salvaging Security When Randomness Fails
84. Security of Data Structures
85. A Physical Design Flow against Front-side Probing Attacks by Internal Shielding
86. ACED-IT: Assuring Confidential Electronic Designs against Insider Threats
87. EOFM-based Clock Reverse Engineering demonstrated on FPGA
88. Firmware Security: Obfuscation and System-level Mutual Authentication
89. Artificial Intelligence Security
90. Attacks on DNN Hardware
91. Automated Assessment of Fault-Injection Attacks at the Pre-silicon: Models, Metrics, and Tools
92. Built-In Self-Authentication (BISA) and Obfuscated BISA to Counter Hardware Trojan Insertion by Untrusted Foundries
93. CAD based solutions to detect and stop optical probing of integrated circuit
94. Design of an on-chip security engine
95. Detecting Zero-day attacks in SoC

96. Electronic Systems Protection throughout the Lifecycle

97. Electronics Supply Chain Integrity Enabled by Blockchain

98. EMFORCED: EM-based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification

99. EOFM-based Clock Reverse Engineering demonstrated on FPGA

100. Firmware Security: Obfuscation and System-level Mutual Authentication

101 FPGA as a Service: Security Challenges and Opportunities

102. Framework for Automated and Systematic Security Assessment of Modern SoCs

103. HARDEN: Hardware-Assisted ML-based Anomaly Detection for Cyber Defense

104. Hardware Trojan Detection Through Information Flow Security Verification

105. Hardware Trojans in AMS domain

106. IoTIC: An Internet of Things Integrity Checker

107. ISIP: A Comprehensive Framework for Information Security for Intellectual Property and System-on-Chip Verification

108. Near-Field EM for Foundry of Origin Identification

109. PCB Trojan Detection and Prevention

110. Protecting Obfuscated Circuits against Attacks that Utilize Test Infrastructure

111. Protection Against Optical Probing Attacks

112. Reverse Engineering of a Neural Network Chip

113. Rowhammer Attack: Desirable or Undesirable

114. Automated Power Side-Channel Leakage Assessment at RTL

115. CAD Framework for Power Side-channel Vulnerability Assessment at Gate Level

116. Secure HDL

117. Secure Software Validation Tools

118. Secure Remote FPGA Initialization in an Untrusted Environment

119. SPARTA: Laser Probing Approach for Trojan Detection

120. Test-chip Design for Security Assessment

121. Universal Security Theory for Evaluation and Design of Nano-scale Devices and for Development of Innovative Security Primitives

123. Authenticated Telephony

124. Characterizing and Strengthening the Modern Health Ecosystem

125. Enhancing Electronic Payment Security

126. Internet of Things Lifecycle

127. Protecting Data with Mandatory Retention Requirements

128. Securing Emerging Digital Financial Systems

129. Securing Machine Learning Systems

130. Development of a Blockchain Oriented Security Class

131. Development of A Hands-on Security Class for Internet of Things

132. Drone-aided Platform for Enabling Next Generation Intelligent Transport Systems

133. Electronic Payments are Essential to Our Modern Economy.

134. Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework

135. An IoT Fingerprinting Framework Using Inherent Device Characteristics

136. Privacy-aware Wearable-Assisted Continuous Authentication Framework

137. Securing Sensory Side-Channels in CPS and IoT Devices and Applications

138. A Sustainable IoT Software Development Framework for Science and Engineering

139. Automatic Author Attribution Via Stylometry

140. A Formal Approach to Deception

141. Hardware/Software Co-Verification for Security

PROJECT DESCRIPTIONS

01. BUILDING A PRIVATE BITCOIN PAYMENT NETWORK USING OFF-CHAIN LINKS

Kemal Akkaya and Selcuk Uluagac

While Bitcoin dominates the market for cryptocurrencies, its use in micropayments is still a challenge due to its long transaction validation times and fees. Recently, the concept of off-chain payments are introduced that led to a payment network called Lightning Network (LN). Off-chain links provide the ability to do transactions without writing to Blockchain. However, design still favors fees and is creating hub nodes that defeats the purpose of Blockchain. In addition, it is still not reliable as not all the transactions are guaranteed to be transmitted to their destinations. If current vendors would like to use it, these problems might hinder its adoption. To address this issue, in this paper we advocate creating a private payment network among a given set of vendors that will serve their business needs, just like the idea of private Blockchains. The goal is to build a pure peer-to-peer topology that will eliminate the need for relays and increase the robustness of payments. Using off-chain links as edges and retailers as nodes, the problem is formulated as a multi-flow commodity problem where transactions represent the commodities from various sources to destinations. As the multi-flow commodity problem is NP-Complete, we not only develop an optimization model but also propose a heuristic approach that utilizes shortest path algorithms in a dynamic way by changing the edge weights as payments are made.

02. DRONE ITS: DRONE-AIDED PLATFORM FOR ENABLING NEXT GENERATION INTELLIGENT TRANSPORT SYSTEMS

Kemal Akkaya and Selcuk Uluagac

The goal of this project is to utilize Unmanned Air Vehicles (UAVs) (or Drones) to not only to enforce the traffic rules and support the traffic police on ground, but also provide the road users with efficient information on traffic (aka intelligent traffic management). ITS UAVs will be enabled by a Dedicated Short Range Communication (DSRC) interface, for Vehicle to Vehicle (V2) and Vehicle to Infrastructure (V2X) communications. In this project, we first lay out the architectural foundations for communication requirements of UAVs by comparing the performance of LTE and mesh solutions in terms of delay and packet delivery ratio. We then looked into connectivity maintenance by introducing a form of minimum connected dominating set (MCDS) problem and how to maintain this MCDS set to keep the network connectivity all the time. Finally, we will also consider security and privacy issues. For security, the main challenge is to enable authentication of the users that will control or communicate with the UAVs. For this, we propose using an existing OAuth 2.0 framework. This will be implemented in the devices. We will then consider privacy of the users when UAVs record video for ITS purposes. To this end, we are considering using FHE for the encryption of video so that it will stay and processed as encrypted in the servers. However, video data is huge and FHE already comes with heavy overhead, so we are exploring to extract background of the videos and only focus on objects in the video to be transmitted.

03. EFFICIENT PUBLIC-KEY MANAGEMENT FOR SMART METER COMMUNICATIONS

Kemal Akkaya

Secure smart meter communications rely on keys for encryption, decryption, authentication, and so on, but management of keys is a challenge. This project addresses public key distribution in smart meter networks, and in particular, how to revoke breached and expired public keys. It aims to develop customized solutions for certificate revocation lists (CRLs) management that will secure the communications in Advanced Metering Infrastructure (AMI) with high efficiency. So far, we investigated Bloom filters, and distributed hash tables to replace the CRL with a more efficient approach. In this project, we propose another novel idea to further reduce the size of CRLs by exploiting Cryptographic Accumulators inspired from Blockchain. The concept provides an efficient mechanism to check whether an element is a member of a specific set. Although cryptographic accumulators provide very efficient membership test (i.e., whitelist), we need a scheme that provides a non-membership test (i.e., blacklist) to allow working with conventional CRLs where a certificate is deemed valid if it is not in the CRL. To enable an accumulator with non-membership proof capability, we construct an accumulator scheme that provides a non-membership witness for each value not in the list. In a nutshell, we propose condensing the entire CRL into single accumulator value to avoid unmanageable CRL size for the smart meters

04. LIGHTWEIGHT SYMMETRIC KEY MANAGEMENT FOR LOW-BANDWIDTH LEGACY ENVIRONMENTS IN SMART GRID

Kemal Akkaya

As the utility companies rightly requests to build the new systems on top of the legacy systems with limited investment, the research community needs to re-think the adaptation of the existing security approaches to such non-traditional legacy environments. This project aims to tackle symmetric key management in a severely constrained communication environment in Smart Grid. Assuming a legacy radio communication infrastructure with bandwidths in the order of kilobits, the objective is not only to reduce the number of messages that need to be exchanged but also minimize the size of the packets that are transmitted. Specifically, we aim to bring Quick UDP Internet Connections (QUIC) protocol of Google in resource-constrained environments by eliminating the need for the PKI. For this purpose, we propose utilizing dynamic key generation techniques that applies cryptographic hash function to a key multiple time so that this can be used for future rekeying without any need for signatures. In this way, we will be able to reduce the number of messages and their sizes significantly. In addition, the scheme lowers communication cost by relieving signature requirement in QUIC. Finally, the scheme also addresses the reliability issues without a need to ACK messages or mechanisms such as the ones used in TCP.

05. MITIGATING ATTACKS TOWARDS NETWORKED CYBER-PHYSICAL SYSTEMS

Kemal Akkaya

Developing security mechanisms for networked cyber-physical systems (NCPS) significantly differs from traditional networked systems due to interdependence between cyber and physical subsystems (with attacks originating from either subsystem), possible cooperation between attackers or defenders, and the presence of human decision makers in the loop. The main goal of this research is to develop the necessary science and engineering tools for designing NCPS security solutions that are applicable to a broad range of application domains. In particular, we experiment traditional DDoS attacks that would result in delaying and packet losses on a two-party NCPS and analyze the behavior on the stability of the control systems. We offer solutions based on game-theory.

06. SDN AND NFV-BASED MOVING TARGET DEFENSE FOR DISTRIBUTED DENIAL OF SERVICE ATTACKS

Kemal Akkaya

One of the recent paradigms to provide security is based on the idea of dynamic networks, which is referred to as moving target defense (MTD). MTD aims to provide agility and/or adaptivity to current networks in order to make it harder for the attackers to launch attacks. Since dynamicity and centralized management is utmost important in applying MTD and forensics, the emerging software defined networking (SDN) and network function virtualization (NFV) can be an excellent technology that can be integrated with MTD and forensics systems for efficient and cost-effective operations. SDN is a key in terms of imposing network-wide policies, upgrades and state changes. This project aims to investigate the potential of SDN and NFV in addressing cybersecurity and resilience for the existing enterprise networks and provide a cost-benefit analysis for all the stakeholders involved in such research and development. In particular, DDoS attacks that aim to congest permanent links are considered. New MTD approaches subordinated with SDN will dynamically change the routes by using the generated fake virtual routes, and direct traffic to internal analyzers. In addition to assessing the overhead of network state changes, we also proposed a signaling game-theoretic model for defender-attacker interaction.

07. VEHICULAR FORENSICS VIA PERMISSIONED BLOCKCHAIN

Kemal Akkaya and Selcuk Uluagac,

Today's vehicles are becoming cyber-physical systems that not only communicate with other vehicles but also gather information from hundreds of sensors within them. These developments help create smart and connected (e.g., self-driving) vehicles that will introduce significant information to drivers, manufacturers, insurance companies, and maintenance service providers for various applications. One such application that is becoming crucial with the introduction of self-driving cars is forensic analysis of traffic accidents. The utilization of vehicle-related data can be instrumental in post-accident scenarios to discover the faulty party, particularly for self-driving vehicles. With the opportunity of being able to access various information in cars, in this project we propose a permissioned blockchain framework among the various elements involved to manage the collected vehicle-related data. Specifically, we will first integrate vehicular public key infrastructure (VPKI) to the proposed blockchain to provide membership establishment and privacy. Next, we will design a fragmented ledger that will store detailed data related to vehicles such as maintenance information/ history, car diagnosis reports, and so on. The proposed forensic framework enables trustless, traceable, and privacy-aware post-accident analysis with minimal storage and processing overhead

08. AUTOMATED REVERSE ENGINEERING OF INTEGRATED CIRCUITS

Navid Asadi, Domenic Forte and Mark Tehranipoor

Deprocessing of ICs historically employs a variety of mechanical and chemical process tools in combination with one or more imaging modalities to reconstruct the IC architecture. In this project, we explore the development of an extensible programmatic workflow which can take advantage of evolving technologies in 2D/3D imaging, distributed instrument control, image processing, as well as automated mechanical/chemical deprocessing technology. Areas as large as 800umX800um were deprocessed on a 65nm node 3.0 cm2 Opteron IC processor chip using gas-assisted plasma FIB delayering. Ultrathinning the silicon substrate in the packaged device within 1-2um of the IC device significantly reduces the amount of time required for deprocessing. The computer aided backside ultra-thinning approach not only improves the success rate, as compared to manual techniques, it also allows the dense lower layers with smallest feature size to be imaged via high resolution SEM first, while the sample layers are the most uniform. Backside deprocessing has the additional advantage that it can be possible to access the device while keeping it “alive” for in-situ electrical testing. Ongoing work involves enhancing the deprocessing workflow with “intelligent automation” by bridging FIB-SEM instrument control and near real-time data analysis to establish a computationally guided microscopy suite. A common python scripting API architecture between the FIB-SEM platform and the image processing and microanalysis platforms permit rapid development of customized programmatic instrument control with data process integration and feedback. We are able to demonstrate, for the first time, tomographic reconstruction based upon automated backside ultra-thinning coupled to automated gas-assisted plasma FIB delayering.

09. NON-DESTRUCTIVE BOND PULL AND BALL SHEAR TESTS FOR ELECTRONICS QUALITY ASSURANCE AND COUNTERFEIT DETECTION THROUGH 3D X-RAY TOMOGRAPHY AND FINITE ELEMENT MODELING

Navid Asadi and Mark Tehranipoor

The lack of trust in foreign and third party entities combined with the prevalence of counterfeit electronics in today's supply chain have increased the need for acceptance tests by the original equipment manufacturers (OEMs) who are responsible for supplying electronic systems in critical applications. Among the many tests, inspection of wire bonds and ball grids are two of the most important. Wire bond related failures contribute to more than 25% of total reliability problems of electronics packages from manufacturing and testing. To perform conventional bond pull and bond ball shear tests, a chip has to be decapsulated either locally or entirely in order to get access to the bond wires. However, this process is destructive and slow. X-ray tomography and Finite element modelling (FEM) can help us speed up the above testing procedure and make it non-destructive. For the first time, we have introduced a new approach based on 3D X-ray tomography and FEM to simulate and analyze the integrity of a real bond-wire without the need to physically decapsulate the chip. This approach enables us to perform a variety of "virtual" tests on the same piece nondestructively.

10. TROJAN SCANNER: DETECTING HARDWARE TROJANS WITH RAPID SEM IMAGING COMBINED WITH IMAGE PROCESSING AND MACHINE LEARNING

Navid Asadi and Mark Tehranipoor

Trojans are malicious changes to the design of integrated circuits (ICs) at different stages of the design and fabrication processes. Different approaches have been developed to detect Trojans namely non-destructive (electrical tests like run-time monitoring, functional and structural tests) and destructive (full chip reverse engineering). However, these methods cannot detect all types of Trojans and they suffer from a number of disadvantages such as slow speed of detection and lack of confidence in detecting all types of Trojans. Majority of hardware Trojans implemented in an IC will leave a footprint at the doping (active) layer. In this paper, we introduce a new version of our previously developed "Trojan Scanner" framework for the untrusted foundry threat model, where a trusted GDSII layout (golden layout) is available. Advanced computer vision algorithms in combination with the supervised machine-learning model are used to classify different features of the golden layout and SEM images from an IC under authentication, as a unique descriptor for each type of gates. These descriptors are compared with each other to detect any subtle changes on the active region, which can raise the flag for the existence of a potential hardware Trojan. The descriptors can differentiate variation due to fabrication process, defects, and common SEM image distortions to rule out the possibility of false detection. Our results demonstrate that Trojan Scanner is more reliable than electrical testing and faster than full chip reverse engineering. Trojan Scanner does not rely on the functionality of the circuit rather focuses on the real physical structure to detect malicious changes inserted by the untrusted foundry.

11. TOWARDS PROVABLY PRIVACY-PRESERVING DATA ANALYSIS WITH PRIVACY FILTERS

Vincent Bindschaedler

Companies routinely want to share sensitive data or data analysis results with the public and other organizations. But due to privacy concerns and legal considerations, such sharing is often limited or prohibited. As a result, there is tremendous desire to find technical solutions, particularly ones that provide formal privacy guarantees such as differential privacy. Existing techniques mostly consist of adding noise to the data (before or after analysis) but this often leads to unacceptable quality loss. This project proposes and explores a novel way to design privacy-preserving algorithms for data sharing and data processing tasks with privacy filters. A privacy filter is a rejection-sampling based technique that systematically identifies and discards outputs or results that leak sensitive information and lead to privacy violations. Our initial work demonstrates the use of privacy filters for sharing sensitive data through data synthesis with arbitrary generative models. Continuing work will explore the use of privacy filters as a general design pattern for privacy-preserving data processing algorithms in various contexts.

12. UNDERSTANDING MACHINE LEARNING LEAKS: CAUSES AND DEFENSES

Vincent Bindschaedler

The increasing popularity of machine learning and AI has unearthed new security and privacy threats. These threats are often due to strange and unexpected behaviors of popular machine learning techniques. For example, deep neural networks often unintentionally memorize (part of) their inputs which allows attackers to maliciously probe these models and extract information about their sensitive training data. This is of particular concern given that companies and organizations increasingly want to share or publish models instead of raw data. Existing solutions such as differential privacy model training do not always scale to complex models without incurring a prohibitive decrease in model performance. Moreover, the extent of the leakage and its root causes remain poorly understood. In particular, preliminary results reveal that overfitting is a sufficient but not a necessary condition for such memorization. The goal of this ongoing project is to understand the fundamental causes of this unintended memorization behavior and eventually to design effective mitigation strategies.

13. ATTENTION BASED SECURE SMART IMAGE SENSOR DESIGN FOR HIGH-SPEED REAL-TIME SECURE VISION APPLICATIONS.

Christophe Bobda

With the increase in image size, sequential image processing on an external processor, and the data transfer time from the sensor to a processor are increasing. Besides, when the sensor sends data, the data confidentiality becomes questionable. Hence traditional commercial CMOS image sensor does not suffice for edge computing where higher resolution and high-speed, secure video processing is inevitable. The goal of this research is to present a secure in-sensor architecture to extract local features in parallel and establish secure communication with an external processor to achieve high acceleration for vision applications. To achieve this milestone, we propose a computational layer in parallel with the image sensor (recently developed by sony). This layer divides the image into several logical regions and has a region processing unit (RPU) for each region. The RPU is a coarse-grain reconfigurable processor and stands to extract local features in parallel. An attention module and a crypto core reside in each RPU. In the attention module, we implement predictive coding, which is observed in our visual systems. It calculates the visual saliency and stands to activate the RPU processing and the crypto core. If the corresponding region has salient information, then the RPU extracts local features, and the crypto core encrypts the data and sends the ciphertext to the external processor. Notably, all crypto cores in the design have different encryption keys to enhance security. Alternately, if a region does not have enough visual information, our architecture skips the data transfer from that region and helps to reduce data volume. The feature data that is transferred is not continuous but discrete. Hence, the design becomes highly secure because of the attention bases system encrypts discrete data with different encryption keys. The external processor then receives the encrypted features and executes the remainder operation in vision applications. Since the processor receives only feature data in a reduced form, the remainder operation can be completed fast on a sequential processor to ensure high-speed processing of a machine vision application. We are currently prototyping the design in FPGA and ASIC platforms. Our future target is to investigate the machine learning algorithms for near sensor processing and develop an architecture to make the sensor more secure.

14. DESIGN OF SECURED MPSOC

Christophe Bobda

Security has become one of the most crucial parts of Multi-processor System-onchip (MPSoC) design because of its usage in the internet of things (IoT) devices, cyberphysical systems, and embedded computing systems. The ever-increasing complexity of on-chip components and long supply chain make SoCs vulnerable to hardware and software attacks. These attacks can be originated either from inside the chip or from malicious software components. To mitigate hardware originated attacks, we propose Hardware Sandbox concept which can be used for secure operation of non-trusted IPs in SoC. Besides, accessing custom hardware IPs in FPGA accelerated SoCs are not controlled by the Operating system. Hence, software originated attacks such as confidential information leakage and denial of service attacks can be launched on those IPs. We propose a hardware isolation approach to ensure controlled access to hardware IPs in the FPGA part of an SoC. The access to an IP is enforced through the Hardware Management Module (HMM) which is a hardware-software co-design and works with the Flask security architecture integrated into the operating system. The benefit of using this security framework is less area overhead and can be easily integrated into the system. We implemented a prototype of our security framework on Zybo Z7-10 with an onboard Zynq SoC with its corresponding petalinux OS image. Currently, we are working on developing the

MeXT-SE tool that can generate platform-independent and secured multi-processor systems from a high-level abstraction. The aim of this work is to ease the implementation of an adaptive multiprocessor system while ensuring security. The proposed design flow starts with a set of abstract and concrete specifications of a system, provided by the user, and ends up generating a generic description of the appropriate hardware design by setting up the communication structure of different components. The resulting abstract architecture is further processed using the vendor tool-chain to generate the target platform's configuration. The generated MPSoC design enforces security by implementing the above mentioned distributed isolation framework to control access of FPGA accelerators in heterogeneous System-on-Chips and is being enforced transparently by the MeXT-SE tool. Our future work focuses on optimizing the MPSoC design considering security in mind.

15. SECURITY IN FPGA ACCELERATED CLOUD AND DATACENTERS

Christophe Bobda

Virtualizing resources within cloud infrastructure offers the opportunity to share physical resources between multiple tenants. As such, the overall performance of cloud services is improved since application codes and data can be co-hosted on single hardware. While computing, network, and storage components such as CPUs, GPUs, memories, and routers have well been exploited in the cloud, FPGA virtualization still needs to be assessed. As a matter of fact, though FPGAs can outperform CPUs and GPUs in several applications, they might also lead to security challenges that can potentially put cloud infrastructures and user applications at risk. Indeed, allowing tenants to share and reconfigure FPGA regions at runtime could result in information leakage, side-channel attacks, denial-of-service, or functional alteration of designs co-deployed on a chip. Therefore, we elaborate an FPGA virtualization approach that emphasizes domain isolation between tasks running in a cloud infrastructure from the software down to hardware threads, preventing applications to access or tamper with the execution of tasks in another's domain.

16. TOWARDS A PRACTICAL AND SECURE FPGA-BASED DIGITAL WALLET

Christophe Bobda

In today's world where a large portion of our assets are in digital form, special precautions must be taken to ensure sensitive materials are safeguarded with protection. Blockchain technology has driven a new trends with cryptocurrency and enables for users a decentralized way to securely manage digital assets and perform transactions between one another. However, the core of security with most digital assets is the protection of one’s keys that limit access to assets to only individuals that hold the cryptographic keys. We set our focus on the development of a more secure and practical hardware wallet for general blockchain assets, with initial attention targeting the Bitcoin cryptocurrency. We propose a hardware wallet based on FPGA that inherits the benefits of hardware implementations while realizing additional FPGA-inherent security measures. We intend to provide the core functionality expected with a wallet in a system-on-chip implementation within reconfigurable fabric, while adding practical features such as wireless BLE communication with a companion application that interfaces with the asset P2P network. Our work has produced an initial prototype hardware wallet on a Zybo Z7-10 with an onboard Zynq SoC and companion mobile application that allows secure Bitcoin transaction signing. We are currently investigating methods for accelerating cryptographic functions with dedicated IP and improving security measures with an SoC implementation that resides solely in programmable logic. Future work aims to expand the scope of targeted digital assets beyond cryptocurrency.

17. INTEL SGX-AIDED SOLUTIONS: FORTIS

Kevin Butler

Intel's Software Guard Extensions (SGX) extend the x86 Instruction Set Architecture with new processor instructions and hardware. SGX provides processor-enforced protected regions of memory, or enclaves, to contain sensitive program code and data. Although enclaves run as user mode (ring-3) applications, other applications and privileged code are prevented from accessing enclave memory. We examine black-box modeling of the enclave, viewing it as a trusted computation oracle. Compared to traditional techniques for secure computation which rely on expensive cryptography, such as garbled circuits and homomorphic encryption, unencrypted computation within an enclave is highly efficient by orders of magnitude. A hybrid scheme combining garbled circuits and SGX is of particular interest, since strong cryptographic guarantees may be needed for the most sensitive portions of programs. We also look at enabling SGX in a practical cloud environment. Containers are lightweight virtualization environments which offer strong security guarantees for the host machine, and they are widely deployed on cloud servers. However, they offer few protections to users. By incorporating SGX, we provide hardware-supported isolation and run-time integrity for user applications running inside containers. Future work will consider other applications of SGX and use of SGX in resource-constrained environments, while revisiting program partitioning and side-channels.

18. ONE-TIME PROGRAMS

Kevin Butler

One-time programs were first proposed by Goldwasser et al. in 2008 as programs that should run exclusively on a single input. Besides the resulting output, nothing else about the program is leaked. Such programs have a variety of applications, ranging from transfer of cryptographic ability to electronic cash and even one-time proofs. A key building block of one-time programs are one-time memories, which (similarly to oblivious transfer) release one of two possible values per bit of input, after which the unchosen value is deleted. We propose using Intel Trusted Execution Technology (TXT) to realize the notion of a one-time memory. TXT provides an integrity-protected environment which is inaccessible from the outside. The core of our program is implemented in garbled circuits (necessary to protect the generator's inputs), but the selection of keys by the evaluator is moved into TXT. Together with the Trusted Platform Module (TPM), TXT supports measured launch for integrity checking, and a sealed flag can be used to satisfy onetimeness. Compared to previous implementations, which relied on highly customized hardware, we aim to make one-time programs practical by using readily available technologies. Continuing work will look at additional applications of and threat models associated with one-time programs.

19. PRIVACY-PRESERVING MULTIPARTY COMPUTATION

Kevin Butler

Secure multiparty computation, also referred to as secure function evaluation, aims to allow multiple parties to learn the output of a function which takes in their private inputs. Nothing more should be leaked besides the final output and what can be inferred from the output. This has typically been achieved with the use of slow and expensive cryptography in the form of garbled circuits or homomorphic encryption. Although these methods have become more efficient over time, they still remain impractical for most real-time, online computations, particularly on modestly-provisioned devices. Additionally, we found flaws in stability and output correctness among the many compilers built for secure computation. Based on these findings, we built Frigate, a garbled circuit compiler that is fully validated using extensive testing and which also greatly outperforms previous circuit compilers. In other work, we tackled the outsourcing of secure computation and efficient representation of circuits. Future work will look at further extension of Frigate. We are also investigating privacy preservation in the dynamic spectrum sensing space. Multiple sensor radios collaborate to localize a transmitting node, but individual sensors should not be linkable back to their measurements. Future work will involve formalizing the security goals and testing alternative protocols.

20. VETTING EMBEDDED FIRMWARE

Kevin Butler

For every visible computer terminal, there are many smaller embedded devices driving everything from user peripherals such as flash drives, mice, and keyboards to internet connected products such as security cameras, thermostats, and home networking equipment. Each separate system runs unique and specialized firmware in order to drive hardware resources, possibly in real-time. Many critical tasks are left to embedded devices, yet many run closed-source software running on top of proprietary or trade-secret hardware. These black-box devices lead to uncertainty and force users to trust the manufacturers and implementers. To regain visibility into normally closed devices, we propose a framework that analyses binary firmware in order to vet it against a set of known security properties. For our first application, we developed FirmUSB to analyze USB device firmware for inconsistencies that could indicate a “BadUSB” attack, which could compromise trusted computer systems at corporations or government offices. To instrument and understand the firmware semantically, we created a binary to Intermediate Representation (IR) lifter, which allows us to understand the compiled code at a higher level of abstraction.

Our future research includes:

- Vetting a diverse range of embedded device firmware

- Supporting additional CPU architectures

- Improving framework performance and robustness

21. AMS CIRCUIT OBFUSCATION

Farimah Farahmandi and Mark Tehranipoor

As the digital circuits, analog and mixed-signal circuits are also susceptible to various attacks such as counterfeit, overproduction, and Trojan insertion. However, unlike digital circuits, the supply-chain security of AMS circuits has not been fully studied. While different logic locking techniques exist for digital circuits, this is not the case for AMS IPs. In fact, analog IPs are the most counterfeited semiconductor product. Therefore, they are the most vulnerable components in a complex system. Due to the low transistor count of analog ICs, that are vulnerable to IP piracy and reverse engineering of their layouts by malicious foundaries. In this project, we will develop a methodology, metrics, and automated tools for obfuscation of AMS IPs to simultaneously meet the security and performance constraints. We will cover two classes of obfuscation solutions, i.e., (1) pure analog blocks (e.g., amplifiers, voltage regulators, current integrators, etc.) and (2) mixed-signal blocks. We will develop an obfuscation process that relies on locking and modification of the digital part for both above mentioned analog IPs. In this project, we will develop analog obfuscation methods and assessment metrics using programmable passives-based methods as well as digital and mux-based locking techniques. We will also establish metrics and a CAD framework for automatic obfuscation and perform a comprehensive security assessment, using both simulation and test chip fabrication.

22. AUTOMATED SECURITY PROPERTY MAPPING FOR LEGACY DESIGNS

Farimah Farahmandi and Mark Tehranipoor

The usage of system-on-chip has been getting a lot of attraction in safety- and mission-critical system. This system requires a strict security requirement due to the fact that the failure of this kind of system causes severe consequences. It has also been shown that security vulnerabilities can be introduced in different stages of hardware design. This leads to the necessity of developing a technique that can ensure security in every abstraction level of the design. Towards this goal, we aim to verify the design against rigorous security properties at every abstraction level of the design. However, one bottleneck is generating security properties for each abstraction level. To mitigate this issue, we will develop an automatic security property mapping framework that translates the security property from one abstraction level to another. The framework helps to reuse the developed security property in one abstraction level to another and greatly reduce the time to regenerate properties for every abstraction level.

23. DEVELOPMENT OF A STATIC SECURITY PROPERTY DATABASE

Farimah Farahmandi and Mark Tehranipoor

With the increasing design complexity of SoCs, it has become very difficult for the design engineers to manually analyze design implementation weaknesses in order to detect vulnerabilities at a lower level of abstractions. Therefore, design houses which are concerned about security, need to maintain a large group of experts to analyze potential security issues. Such a manual approach is both time-consuming and expensive. All these issues highlight the necessity for generating a comprehensive set of security properties that a design must hold to pass security assessment. In this project, our goal is to develop an architecture agnostic static security property database, based on different security assets in various design abstractions and probable vulnerabilities which the assets can encounter during design and deployment stages. Verification engineers can map the security properties from the database into assertions and feed the assertions to different formal (e.g., equivalence checker, theorem prover, model checker) and simulation-based approaches to perform security verification and validation. Moreover, design engineers can use the database as a guideline to ensure security in the design stage. The security property database will be utilized to develop security metrics for security evaluation of design, both quantitatively and qualitatively. The coverage and severity of the identified security properties can be used as metrics for security verification closure. For a design with weak security, a designer can go back and modify the design to address the detected security vulnerabilities.

24. FPGA BITSTREAM REVERSE ENGINEERING-BASED DEVICE UPGRADE

Farimah Farahmandi, Fahim Rahman and Mark Tehranipoor

Field Programmable Gate Arrays (FPGAs) are widely deployed in numerous mission-critical systems, such as cloud infrastructures, aerospace, and military applications, due to their reconfigurability and short time-to-market. For higher security and performance, there are practical requirements for upgrading the FPGA devices that remain in the field for many years to more advanced ones. However, the source code of the old FPGAs may not be available today because of the poor management, which hinders the upgrade of the devices. Therefore, it is crucial to find a way to recover the functionally equivalent synthesizable RTL (register-transfer-level) code from the bitstreams of the obsolete FPGAs. In this project, we will study the FPGA architecture of various Xilinx FPGA families and the compositions of corresponding bitstreams (note that the bitstream format is proprietary and undocumented). Next, we will propose schemes on how to reverse engineer bitstreams to their functionally equivalent RTL code and then resynthesize the code to migrate the same design to the new devices. Finally, we will develop a tool to upgrade the devices automatically.

25. FPGA TROJAN DETECTION USING STATIC DESIGN ANALYSIS

Farimah Farahmandi and Mark Tehranipoor

Nowadays, Field Programmable Gate Arrays (FPGAs) have already served as the reconfigurable hardware platforms for various applications, ranging from low-cost consumer electronics to high-end military systems. However, the security concerns regarding FPGA devices are increasing because hardware Trojans can be inserted into them, not only at the design/fabrication phases but also at deployment stages by tampering configuration bitstreams. Dynamic detection methods like side-channel analysis always call for golden models, and they may not be effective if the Trojan is very tiny. On the other hand, code/netlist-based static detection methods show a promising direction to address FPGA Trojan threats since they can analyze the features of the whole design directly. Nevertheless, in most cases, only the low-level binary FPGA bitstream files rather than high-level code/netlist are available. Therefore, in this project, we will recover the high-level design information (code/netlist) from FPGA bitstream. Also, we will develop efficient FPGA Trojan detection schemes to identify the malicious logics hidden in the recovered design.

26. HARDWARE OBFUSCATION USING HLS

Farimah Farahmandi and Mark Tehranipoor

High-level synthesis (HLS) has been proven to be an effective solution to address the ever-growing demand for increasing design and verification productivity of the semiconductor design flow. Being extensively matured since its introduction, HLS provides a superior capability to raise design abstraction and produce hardware-independent design specifications with less complexity for ASIC and FPGA implementations. There are fundamental differences in code execution, management of variables, and control flow between high-level languages and translation tools. These differences facilitate a huge scope to obfuscate designs to make it more robust against conventional attacks. A higher abstraction model can be beneficial in blending the key in the control flow better, and the number of optimization levels will increase, which can mask the sensitive details of the design better. Also, data flow can be made implicit if necessary, using combined techniques in the higher abstraction, which was not possible at the gate level. In this project, we are working on testing cases of different techniques for inserting keys into different entry points of C/C++ codes and evaluating the performance in terms of overhead (area, power) and attack resiliency. The final goal is to identify the best way to obfuscate the higher-level abstraction and create specific rules that need to be followed for it.

27. IDENTIFYING VULNERABILITIES INTRODUCED BY HIGH-LEVEL SYNTHESIS

Farimah Farahmandi and Mark Tehranipoor

High-level synthesis (HLS) has gained much popularities in recent years as it significantly reduces time-to-market by directly translating codes developed in high-level software language, e.g., C to synthesizable hardware designs. Although there have been many works on improving the high-level synthesis process (in terms of performance, area, and power), none have investigated potential security vulnerabilities introduced by HLS. In this project, we are investigating vulnerabilities introduced by the HLS, which could be exploited by attackers to gain access to the assets in hardware design. Our objective is to identify the coding practices and HLS settings, which leads to security vulnerabilities and then develop a guideline to guide design engineers what to do (Do-s) and not to do (Don'ts) during high-level design implementation and HLS.

28. INFORMATION FLOW TRACKING BASED SOFTWARE VULNERABILITIES DETECTION

Farimah Farahmandi, Fahim Rahman and Mark Tehranipoor

Buffer and integer overflow vulnerabilities and exploitations pose major security threats in the modern computing era. For example, buffer overflow alone accounts for approximately half of prevailing security vulnerabilities. Such vulnerabilities cause arbitrary code executions, denial of service attack (DoS), unauthorized accesses, and the leakage of secret information to unauthorized parties. However, there is a scarcity of efficient and static formal analyzers for software vulnerabilities detection; instead of some run-time solutions are available. The existing run-time solutions overlook most of the practical scenarios of buffer and integer overflow cases. At the same time, they also create large memory overhead with reduced performance and verify only a few execution paths. As a result, the existing solutions are not suitable, especially for low-end embedded systems. In this project, we develop an efficient solution to detect the critical buffer and integer overflows. We integrate the dynamic information flow tracking along with the formal verification (model checking) approach. In the scheme, while the information flow tracking technique tracks untrusted data that are used in array index/loop bound (which may cause Buffer Overflow or Integer Overflow), the model checker traverses all possible paths to find out all critical vulnerabilities and provides formal proof of vulnerabilities in static time.

29. METRIC-DRIVEN SECURITY PROPERTY VERIFICATION

Farimah Farahmandi and Mark Tehranipoor

Security of a system on chip (SoC) can be weakened by exploiting information leakage, timing and power side-channel attacks, design-for-test (DFT) structures, faultinjection attacks, malicious modification during design and manufacturing process, etc. Apart from the vulnerabilities exposed by these attacks, many security vulnerabilities in SoCs can be unintentionally created by designers' mistakes and the designers' lack of understanding of security issues and unsafe design practices. Moreover, computer-aided design (CAD) tools can introduce additional vulnerabilities in the SoCs while performing power and performance optimizations. These vulnerabilities creates an increased need for a comprehensive security verification and validation efforts. In this project, we develop metrics for quantitative security assessment in the pre-silicon design stage. Depending on security assets, design attributes, associated vulnerabilities, and potential threats, as well as abstraction levels (e.g., RTL, Gate level, Layout), that can be used for security verification and validation.

30. SECURITY VERIFICATION OF AI SYSTEMS

Farimah Farahmandi

With the prevalence of machine learning algorithms, there will be more and more SoCs that contain a dedicated AI accelerator. Compared to traditional SoCs, neural engines improve the intelligence of SoCs and open more backdoors for security issues as well. There may be a limited control on what AI systems learn and policies they internalize in their learning process. AI learns a task through objective functions. Defining objective functions to reflect security concerns and verification is of high importance. If the objective function does not cover all aspects of security requirements and the correct functionality, there is a chance that AI learns vastly different concepts and ends up in unwanted situations. Further, AI may internalize some sensitive information which is decodable by reverse engineering. In this project, we propose designing new policies and quantitative methods to measure the level of trust of the design. We also propose new validation solutions using combining formal methods and test generation techniques to verify security properties of the design.

31. SECURITY VERIFICATION USING FORMAL METHODS

Farimah Farahmandi

With the globalization of the IC industry, the outsourcing and integration of third-party hardware Intellectual Property (IP) blocks have become a common practice for System-onChip (SoC) design. However, it raises significant security concerns as an attacker can insert malicious components in third-party IPs and tamper the system. Therefore, using the conventional validation method is not effective in detecting malicious functionality. From the security point of view, it is important to prove that the design implementation is equivalent to its specification, nothing more, nothing less. However, existing formal methods can lead to a state-space explosion when complex and large IPs are involved. In this project, we develop efficient, formal techniques to identify various potential threats in third-party IPs, analyze their vulnerabilities using theoretically defined metrics, and formally detect them. In this research, we effectively utilize three widely used formal methods (equivalence checking, model checking, and theorem proving) for scalable security validation.

32. SERFI: SECURE REMOTE FPGA INITIALIZATION IN AN UNTRUSTED ENVIRONMENT

Farimah Farahmandi and Mark Tehranipoor

The functionality of an FPGA is completely defined in its binary configuration bitstream. The bitstream is often protected by encryption. The encryption key, as a root of trust, is stored in the non-volatile memory inside the FPGA to defend against various attacks like bitstream reverse engineering, tampering, and cloning. For low cost and short time-to-market, trusted system designers often rely on a potentially untrusted system assembler to buy components, assemble the system and share the encryption key to load the bitstream into the FPGA. However, since the assembler is untrusted, the key sharing process may result in secret leakage and thus the security of the entire bitstream is threatened by enabling attacks such as hardware Trojan insertion and bitstream tampering. Therefore, it is important to guarantee the security of sharing the encryption key between the trusted designers and the FPGAs through untrusted assemblers. In this project, we will propose the communication protocol which can transmit the encryption key securely from a trusted system designer into an FPGA in physical possession of an untrusted system assembler.

33. SECURITY-PRESERVING POST-SILICON VALIDATION AND DEBUG

Farimah Farahmandi and Mark Tehranipoor

Due to the stealthy nature and practically infinite space of malicious functionality as well as design complexity and shrinking time-to-market, a cleverly inserted malicious functionality in a large SoC is highly likely to evade conventional post-silicon validation approaches. In this project, we propose novel post-silicon security validation techniques to ensure the security and trust of silicon designs based on coverage analysis, penetration tests, and data analysis. Currently, there is no effective way to collect coverage of security properties and requirements directly and independently on silicon. We explore how to utilize on-chip design-for-debug infrastructure effectively (e.g., trace buffer and scan chain) to improve the observability of security properties while preserving the confidentiality requirements of the design. There is an inherent conflict between increasing observability and security. We also propose secure architectures for design-for-debug that do not violate any security constraints by effectively utilizing information flow tracking as well as sidechannel analysis. Moreover, this project aims to explore scrambling and encryption methods to protect the data stored in the trace buffers to prevent information leakage.

34. AGING-RESISTANT FPGA RO PUF

Domenic Forte

Temporal variations like temperature, supply voltage and environmental noise, and silicon aging make it challenging for physical unclonable functions (PUFs) to produce reliable signatures. In the case of FPGA, the problem is even worse since the internal architecture of FPGA is a black box where layout/gate level design alterations are out of the user's hands. Though aging resistant ring oscillator (RO) PUFs have been proposed previously for ASIC design, implementing the same techniques in FPGA is impossible as it involves redesigning the circuit at transistor level. In this project, we are developing the first aging resistant RO PUF design on FPGA. Our approach exploits unused resources in FPGA look up tables (LUTs) to (i) reduce aging degradation and (ii) increase the homogeneity in RO aging. By improving PUF reliability, we can also reduce the hardware overheads and signature leakage resulting from implementations of error correcting codes (ECC). Initial experiments from Spartan 3A FPGA boards demonstrate that our proposed RO PUF is less affected by aging, with the reliability increasing by 37.4% on average. Moreover, by comparing our design with conventional RO PUF in FPGA, the aging degradation decreases by 37% as well.

35. ATTACKS AND COUNTERMEASURES FOR SEMICONDUCTOR IP PROTECTION

Domenic Forte and Mark Tehranipoor

Semiconductor intellectual property is undoubtedly one of the most valuable assets for any electronic design company, requiring enormous amounts of time, monetary investment, research, and development. However, such IPs can be compromised at various steps in the design process, most notably during fabrication at an untrusted foundry, and in the supply chain by reverse engineering attacks. Logic encryption has emerged as a promising solution that enables an IP owner to 'lock' their IP so that unauthorized parties are unable to engage in piracy or theft. However, such techniques are vulnerable to a wide array of attacks that either circumvent the locking mechanism or compromise the key required to unlock the IP or IC. In CHES '17, we showed that such locking techniques, in spite of being secured by key protection techniques, are vulnerable to functional circumvention or bypass attacks. In light of this and numerous concurrently proposed attacks, we have identified binary decision diagrams (BDDs) as an appropriate framework for evaluating logic locking against different attacks. Our current work in this domain revolves around (i) functional locking techniques with BDD at RTL and netlist levels; (ii) evaluating trade-offs in overhead vs. security, (iii) extending combinational locking techniques to sequential circuits, and vice versa.

36. AUTOMATED COUNTERFEIT IC DEFECT DETECTION

Domenic Forte, Mark Tehranipoor, Navid Asadi and Damon Woodard

In the past decade, electronics counterfeiting has reached a new level of sophistication. With improved replication techniques and the growing reliance on electronic systems worldwide, the possibility of important systems becoming compromised increases every day. In 2011, it was revealed that the Navy's submarine hunter aircraft had compromised ice detection systems. Additionally, in 2014, the Navy's nuclear submarines were discovered to use counterfeit electronic parts. Because these parts can allow backdoor access, it becomes prudent to vet the parts being used in important systems. Standard procedures involve manual examination of parts for defects by an SME, which can be expensive, time-consuming and destructive. With the goal of automating the entire process, we have initially focused on surface defects, which are easier to detect with image processing techniques. Using the Leica DVM-6, we can quickly generate large databases of images to process. We developed an algorithm to register images obtained so they had the same chip orientation and positioning. So far, we have ad hoc techniques to detect scratches, texture differences on the surface of the chip, displacements in the identification marking locations, and color variations. We're currently developing approaches based on neural networks to identify scratches in images, and the eventual goal is to develop an entirely automated process that can analyze whole trays of chips at once.

37. AUTOMATED NON-DESTRUCTIVE PCB REVERSE ENGINEERING FROM X-RAY COMPUTED TOMOGRAPHY

Domenic Forte, Mark Tehranipoor, Navid Asadi, and Damon Woodard,

In the modern globalized supply chain, reverse engineering (RE) is needed to validate the performance, quality, authenticity, and integrity of electronics, e.g., detection of counterfeits and hardware Trojans. In the case of legacy systems, RE can be an invaluable tool for recovering original design files in order to evaluate, reproduce, and/or redesign them. The goal of this project is to develop an entirely automated and non-destructive process for the reverse engineering of printed circuit boards (PCBs). X-Ray computed tomography is used to capture a 3-dimensional scan of the entire depopulated board, both external and internal layers. Afterwards, the resultant images are then subject to advanced image processing and machine learning algorithms to intelligently extract the boards' via and trace schematic features. Once the features have been classified and localized, the schematic undergoes vectorization to translate the features from a pixel related information to geometrical information, such as diameter of vias and width of traces. Lastly, the vectorized board information is then exported to a DXF file for the board to be analyzed and/or fabricated. As part of this project, we are currently investigating accurate methods to classify traces and vias, remove noise from presence of high-Z material on the PCB, etc. In future work, we will extract automatically extract component information from optical images of the PCB as well as extend our work on X-ray to populated PCBs.

38. BLOCKER: A BIOMETRIC LOCKING PARADIGM FOR IOT AND THE CONNECTED PERSON

Domenic Forte and Damon Woodard,

Biometric techniques offer major advantages over conventional identification and authentication methods, particularly, they are more secure, accurate, reliable, and user-friendly. Nevertheless, they suffer from limitations associated with protecting users' biometric templates against various attacks, e.g., template theft, illegal system access, etc. Unfortunately, existing countermeasures are also extremely limited. This motivates us to develop a framework called BLOcKeR - Biometric Locking by Obfuscation, Physically Unclonable Keys, and Reconfigurability, which combines biometrics and configurability with two recent advances in hardware security, namely physically unclonable functions (PUFs) and hardware obfuscation. In this regard, a PUF - an object's fingerprint - is incorporated to tie a device (i.e., an integrated circuit) to the biometrics of its owner. Moreover, hardware obfuscation is used to "lock" the hardware from the gates up to the firmware such that it behaves inappropriately without a biometric-dependent key. Besides unique benefits such as configurability and non-linkability, BLOcKeR requires no template storage, contrary to traditional biometric systems. These enhancements make BLOcKeR resistant to various attacks, according to our security assessment. As a first step, we have considered enrollment of a device to one user, whereas our future work shall focus on extending BLOcKeR to multi-user environments (e.g., the family laptop).

39. CARDIOVASCULAR BIOMETRIC AUTHENTICATION, KEY GENERATION, AND PRESENTATION ATTACKS

Domenic Forte and Damon Woodard

Cardiovascular signals, such as electrocardiogram (ECG) and photoplethysmograph (PPG), have been investigated as biometrics for the last decade and owe their initial popularity to anticipated spoofing resistance. In this project, we have investigated the following: (1) Methods for secure and reliable ECG-based key generation – our approaches quantize ECG signals into keys based on tunable reliability and entropy parameters. To reduce the need to enroll users over long periods of time and conditions, we also model various noise sources affecting ECG. Our approaches have achieved keys with lengths 300-500 bits for normal ECGs and 98% key reproducibility; (2) First investigation of PPGbased human authentication and recognition based on non-fiducial features; (3) First ever presentation attacks on ECG-based biometric systems – in over 2,500 simulation experiments, our approaches successfully spoofed ECGs 96.7% and 91.78% of the time for fiducial and non-fiducial feature extraction methods and with only one heartbeat of the victim; and (4) Obfuscation-based biometric systems – to protect biometric templates/systems from theft and fault injection, we are using biometric keys to lock/unlock hardware obfuscated systems. In future work, we plan on implementing our quantization methods and presentation attacks in FPGA, reducing the cost of ECG pre-processing through better understanding of noise, and developing countermeasures to ECG presentation attacks.

40. CIRCUIT EDIT ENABLED TRUSTED FABRICATION FOR LOW VOLUME PRODUCTS

Domenic Forte, Mark Tehranipoor, and Navid Asadi

The modern trend of off-shoring semiconductor foundries has led to a decrease in costs and turn-around time for state-of-the-art IC designs. However, this has also created lack of control and trust in the fabrication process, with threats such as IP piracy and Trojan insertion arising as serious concerns, especially for critical applications such as aerospace and military. In order to mitigate such threats, various design protection schemes against an untrusted foundry have been proposed. However, they suffer from high costs, non-trivial overheads, and new attack vectors. Towards this end, we are investigating new techniques that leverage post-fabrication circuit edit for design obfuscation and low-volume trusted fabrication. In this approach, gate-level netlists and layouts are modified and an obfuscated design is fabricated at the untrusted foundry. Circuit edit technologies, along with appropriate layout features, are then used to recover the intended functionality of the design at a trusted facility, thereby preventing the foundry from pirating the design. Initial design obfuscation techniques were presented at ICCAD '16, where we showed that it is possible to make minimal changes to the design with circuit edit constraints, while ensuring that an untrusted foundry is unable to identify the changes made. We are now currently investigating reliability issues that may arise due to circuit edit - by performing focused ion beam (FIB) modification on chips fabricated at advanced nodes, and how to mitigate them a priori during the design stage.

41. COVERT GATES: PROTECTING INTEGRATED CIRCUITS FROM REVERSE ENGINEERING WITH UNDETECTABLE CAMOUFLAGING

Domenic Forte and Mark Tehranipoor

Existing methods of camouflaging are based on logic gates that assume one of many Boolean functions, either through variation of threshold voltage or contact configurations. Unfortunately, such methods lead to high overheads, and are vulnerable to invasive as well as non-invasive functional attacks. We have developed a new camouflaging strategy, termed as 'covert gate', that leverages doping and dummy contacts to create camouflaged gates that are indistinguishable from regular gates under modern imaging techniques. The technique allows a designer to introduce arbitrary dummy inputs to logic gates, so that the netlist retrieved by the attacker during reverse engineering is functionally incorrect. Since covert gates are indistinguishable from regular gates, attack complexity is significantly increased and with very low overheads. In preliminary work, we have fabricated and imaged test structures to show the indistinguishability of the channel and contact regions that are modified to create covert gates. Our empirical results show that covert gate indistinguishability can make SAT attacks exponentially more complex and prevent gate identification by ATPG-based attacks even under pessimistic assumptions. We have also developed models to characterize gate-level overheads, and netlist modification tools for camouflaging designs. In the future, we plan to fabricate prototype devices to validate our models, estimated overheads, and indistinguishability of gates in silicon. We also plan to improve our covert gate insertion methods to meet different objectives (minimize area, performance, or power overheads, maximize security, etc.).

42. DEVELOPING LOW COST ELECTRICAL TEST METHODS FOR COUNTERFEIT FPGA DETECTION

Domenic Forte and Mark Tehranipoor

Counterfeit components do not possess the same specifications as genuine parts, and can impose significant vulnerabilities and threats to the systems in which they are placed. Reports show that recycled and remarked ICs comprise 80% to 90% of all counterfeits in circulation worldwide. Hence, significant work has aimed to develop low cost and less time-consuming electrical test methods to detect such counterfeits. Programmable ICs are in top 5 counterfeit list and FPGA holds a good portion of it. In this project, we have developed effective test methods for recycled FPGA detection based on supervised and unsupervised machine learning algorithms. We developed a sophisticated ring oscillator design and voltage scaling based fingerprint of FPGA logic cells to exploit degradation. The unsupervised method requires very little (if any) golden information and is effective in the case of legacy chips. We examined the proposed methods for Spartan-3A and Spartan-6 FPGAs, and the result shows that both methods can detect most recycled FPGAs which have experienced accelerated aging for at-least 12 hours. In future, we plan on extending our approaches for detecting remarked FPGAs.

43. EMFORCED: EM-BASED FINGERPRINTING FRAMEWORK FOR COUNTERFEIT DETECTION ON REMARKED AND CLONED ICS

Domenic Forte and Mark Tehranipoor

Counterfeit detection techniques often suffer from high cost, device overhead, and testing time. EMFORCED introduces an electromagnetic-based counterfeit detection framework which can be utilized by several entities with no prior knowledge of the devices under test. As our method does not require test vectors, but rather relies on extracting an electromagnetic fingerprint from the circuit only excited by clock, power, and ground inputs. By utilizing statistical analysis methods and machine learning techniques, we demonstrate high-accuracy classification with, or without, a golden reference. EMFORCED offers a low-cost, fast, and zero overhead solution to differentiating between designs.

44. EMFORCED: EM-BASED FINGERPRINTING FRAMEWORK FOR REMARKED AND CLONED COUNTERFEIT IC DETECTION USING MACHINE LEARNING CLASSIFICATION

Domenic Forte and Mark Tehranipoor

Electronics supply chain vulnerabilities have broadened in scope over the past two decades. With nearly all IC design companies relinquishing their fabrication, packaging, and test facilities, they are forced to rely upon companies from around the world to produce their ICs. This dependence leaves the electronics supply chain open to counterfeiting activities. EMFORCED, an electromagnetics-based fingerprinting framework, is designed to detect remarked and cloned counterfeit ICs. Benefiting from naturally occurring electromagnetic second order effects to identify the IC design layout without decapsulating the chip under test. Enabling only the clock, power, and ground pins allows us to generate a designspecific fingerprint which is dependent upon the physical parameters of the chip under test. Leveraging the emissions from the clock distribution network creates a holistic, designlevel, fingerprint including both temporal and spatial information. Statistical analysis and machine learning techniques are used to demonstrate reference-free and referenceinclusive classification methods based on EMFORCED measurements, providing various scenarios for this low-cost, fast, and zero design overhead solution.

45. FORTIS: ESTABLISHING FORWARD TRUST FOR PROTECTING IPS AND ICS IN TODAY'S COMPLEX SUPPLY CHAIN

Mark Tehranipoor , Domenic Forte, Fahim Rahman, and Farimah Farahmandi

Growing complexity of system-on-chip (SoC) and ever-increasing cost of IC fabrication have forced the semiconductor industry to shift from a vertical business model to a horizontal model. In this model, most entities involved in SoC design flow are located across the globe and original intellectual property (IP) owners do not have the ability to monitor and control the SoC design flow. The lack of trust and transparency/ control has led to vulnerabilities such as IP piracy, IC overproduction, etc. The main objective of this project is to develop a comprehensive framework, named FORTIS for detection and prevention of all the mentioned supply chain issues. We have completed the following tasks for the implementation of FORTIS framework,

1. Developed and implemented attack-resistant logic obfuscation techniques
2. Developed and implemented a locking mechanism which enables structural testing without the need of activating the chip
3. Developed and implemented a locking mechanism which enables structural testing without the need of activating the chip
4. Developed a hybrid mechanism of IP encryption and logic obfuscation to prevent IP tampering, cloning, and overuse
5. Developed the concept of Trusted Authentication Platform (TAP) to address issue like recycling, remarking, and out-of-spec/defective ICs
6. Secure key exchange for IC/IP metering

Future research plans:

1. Implement logic obfuscation techniques which is resilient to state of the attacks e.g., SAT attack
2. Implementation of the TAP module
3. Implementation of unique key for every chip

46. HIERARCHICAL BLOOM FILTER (HBF) FRAMEWORK FOR SECURITY, SPACE-EFFICIENCY, AND RAPID QUERY HANDLING IN BIOMETRIC SYSTEMS

Domenic Forte and Damon Woodard

Due to the proliferation of IoT devices in numerous human interactive applications, there is a surge in biometric data collection and analysis. Maintaining and using such databases has challenges related to local storage requirements, long query times for data mining, threats to user privacy, and denial of access due to the presence of noise in the biometric input queries. We have developed a Bloom Filter (BF) based approach that addresses storage-efficiency, fast query-processing, security, and fuzziness issues altogether in a single approach. BFs have linear search time and storage. Further, secure one-way hashes used by the BF can provide security to the biometrics it stores. However, legacy BFs cannot handle noisy data, i.e., a single bit flip in a biometric template can cause havoc in the BF operation due to the one-way functions. In our research, we have proposed a hierarchical BF (HBF) based framework that is tuned to desired false positive / false negative (FP/FN) rates based on noise characteristics of the data. An HBF involves multiple levels, each with multiple BFs that store part of the biometric template. In our proposed approach, if a pre-defined number of BFs from the HBF (determined analytically based on desired FP/FN rates) can authenticate the noisy biometric query, then the template is considered as contained within the database. Our proposed architecture has been implemented using a face database containing 30,000 facial templates and achieves 12x reduction in storage size with 570x reduction in average query time without sacrificing accuracy. In ongoing research, we are investigating (i) the best feature representations for the HBF templates, e.g., LBP, PCA, CNN, etc.; (ii) improving biometric quantization schemes; (iii) examining the effectiveness of tampering, collision, etc. attacks on the HBF; and (iv) studying the impact to storage savings and attack surfaces when FP/FN parameters are relaxed.

47. INTRINSIC MEMORY-BASED SOLUTIONS AGAINST COUNTERFEIT ICS

Domenic Forte and Mark Tehranipoor

As the consumer electronics market continues to expand, counterfeit electronics have become more profitable and difficult to contain. The most prevalent type of counterfeit in the market is “recycled” (i.e., used and resold as new). Existing approaches detect recycled ICs add aging sensors to the design, and therefore induce undesired area/power overheads. Other techniques, such as light emission and dynamic current analysis have been exploited, but require a golden model. Seeing these drawbacks, we are investigating zero-overhead solutions based on SRAM, DRAM, and Flash memory primitives. Our solutions can be exploited to detected recycled standalone memory components as well as such ICs with embedded memories. The SRAM primitive involves identifying aging sensitive start-up behavior to detect recycled SRAMs. Using a statistical inference approach, we have been able to achieve a high detection accuracy (> 96.5%) and promising sensitivity (> 7 hours in-field usage). DRAM solutions are part of ongoing work, but follow a similar methodology. Our Flash based primitive exploits partially programming, and an aging model is constructed by analyzing the failures which are induced by it. Our preliminary experiments achieved a 100% detection accuracy for Flash used by as little as 5% of its endurance. In addition to recycled IC detection, we are also developing methods to generate unique identifiers based on process variation from SRAM, DRAM, and Flash with bit error rates on the order of 10-5 or better. Such IDs can be used to detect or prevent remarked, cloned, and overproduced counterfeit types.

48. METRICS AND BENCHMARKING FOR LOGIC LOCKING AND HARDWARE OBFUSCATION

Domenic Forte and Mark Tehranipoor

For IP vendors and IC design houses, reverse engineering is a major threat resulting in piracy and/or modification. To protect against it, hardware obfuscation is a technique that can provide sufficient security with minimal modification of the design flow. It is the process of concealing the design from an adversary by removing understandability. Obfuscation is an active field of research in hardware security community and the increasing amount of interest in the field demands the proper evaluation and comparison platform among the techniques. We are developing the first hardware obfuscation benchmarks which can be used as standards for that purpose. Our initial set of IC benchmarks is obfuscated using inhouse and popular approaches from the literature, different key sizes, and different countermeasures. The benchmark suite has already been made available in TrustHUB website and constantly being upgraded. The website also contains a taxonomy, naming convention, and format for others to follow in order to submit their own benchmarks. Using our benchmarks instead of arbitrary circuits in research publications will facilitate a uniform comparison of existing and new innovations. In our current work, we are also formulating a set of metrics that indicate distinct aspects of an IP that makes it more secure or vulnerable against known attacks.

49. NANOPYRAMIDS - OPTICAL SCRAMBLERS FOR PROTECTING AGAINST BACKSIDE PROBING ATTACKS

Domenic Forte, Mark Tehranipoor and Navid Asadi

Originally used for failure analysis, optical probing techniques, such as photon emission microscope (PEM) and laser voltage probing (LVP), now enable an adversary to probe volatile and on-die-only secret data from an integrated circuit without making physical contact with transistors and interconnects. Recent attacks have demonstrated that secret keys and decrypted configuration data can be successfully localized and optically probed from Static Random Access Memory (SRAM) or Field Programmable Gate Arrays (FPGAs). Existing countermeasures against the attacks come with significant shortcomings such as manufacturability, area overhead, and fabrication cost. Here we propose a novel nanoscrambler device structure as an efficient countermeasure technique. Nanopyramids are introduced between the transistor layer and the first metal layer to randomly scatter the light that carries sensitive information. Our simulations have shown that the pyramid structure causes significant light scattering. The signal collected by the adversary from the collecting spots no longer deliver the data in the gates on the same spots, resulting in unsuccessful data interpretation and attack failure. The benefits of this technique include the compatibility with standard CMOS processing, working in passive mode, and zero area overhead. Tasks for the future research will be: (1) complete device modeling and characterization; (2) prototype device fabrication; and (3) demonstration of attack failure in silicon.

50. OBFUSCATION-BASED PCB ANTI-REVERSE ENGINEERING

Domenic Forte

Printed circuit boards (PCBs) provide mechanical support and electrical connections between electronic components and chips. Modern PCBs are complex, multi-layer structures that contain critical design information and intellectual property (IP), but are virtually unprotected. PCBs suffer from threats such as cloning, overproduction, and unauthorized operation. Cloning refers to the reverse engineering of the PCB in order to reproduce an unauthorized copy. Overproduction refers to the case where a contract foundry, who possesses the detailed PCB design, produces more PCBs than authorized to. Existing protection approaches focus only on how to prevent attackers from learning secret information of a device during operation, but do not address these issues directly. To migrate these threats, we are investigating PCB obfuscation methods that obscure the design information from attackers. Our approaches physically hide inter-chips connections with a chip added to the PCB and/or under protective opaque materials. We have applied our framework on several industrial reference designs, and found that the time required to break it is as longer than hundreds of years. We are currently investigating alternative attacks and countermeasures based on semiconductor aging, probing, stream ciphers, and formal test methods.

51. PCB TAMPER DETECTION

Domenic Forte

Re-routing internal paths and adding components on printed circuit boards (PCBs) makes it possible to bypass the copyright verification, break the carrier restriction, and run 3rd-party systems. The primary method of achieving these goals is to install a modification chip (mod-chip) into the system. A mod-chip is a small electronic device used to alter or disable artificial restrictions of computers or entertainment devices (e.g., videogame consoles, Blu-ray players, etc.). Physical countermeasures have been proposed to address this attack. For example, PCBs can be protected in a hard steel case with tamper evident switches that activate to suspend the system if the case is opened. Vibration sensors can be used to monitor abrupt movements. However, these solutions present some drawbacks. To eliminate tampering attacks, we are investigating approaches that rely on capturing unclonable signatures in the PCB traces based on process variation. Our initial modelassisted PCB attestation framework monitors the changes in trace impedance introduced by tampering of critical board-level interconnections with board-level ring oscillators. A preliminary implementation that runs a detection phase prior to the normal PCB operation was able to detect tampering events with more than 99.92% accuracy.

52. A PROVABLE-SECURITY TREATMENT OF COUNTERFEITING PROBLEMS IN ELECTRONICS SUPPLY CHAIN

Domenic Forte and Thomas Shrimpton

A counterfeit electronic component is an electronic part that deviates from a legitimate part in terms of ownership, specification, functionality and performance. Counterfeiting of electronic parts is a multi-billion dollar industry. Hardware obfuscation techniques have been proposed to curb this problem. However, these techniques often use cryptographic primitives and protocols in an ad hoc fashion, without the guidance of the "provable security" framework that underpins modern cryptography. Within this framework one first develops precise descriptions of the primitive that one needs to design (the "syntax"), then establishes formal notions of security for the primitive, i.e. the attack model and the security goal that the primitive targets. These steps make it clear what one needs to instantiate, and provide a way to say, definitively, whether or not a particular instantiation is secure. In this project, we aim at providing a comprehensive provable-security treatment to the problem of electronic part (e.g. chip) counterfeiting. This is a multifaceted problem. As such, we will be developing precise syntax and security notions for things like obfuscated chip-designs (a common approach to preventing counterfeiting), chip-verification protocols, and overproduction-prevention schemes. We will analyze existing approaches relative to our syntax and notions, in order to understand the attacks against them, and then leverage this understanding to build new, provably secure approaches.

53. RASC: ENABLING REMOTE ACCESS TO SIDE-CHANNELS FOR MISSION CRITICAL SYSTEMS

Domenic Forte and Mark Tehranipoor

Traditionally side-channels such as power and EM have been limited in scope as the system under test has been restricted by physical access. Here we introduce RASC, an embedded system with a footprint of approximately 2 square centimeters which can record, process, and transmit side-channels from a remote system. RASC is designed to be deployed within a system and have access through either power or EM side channels depending upon the application and system requirements. Trusting this secondary system provides trust within the system under test and requires no overhead within the current design, thus it is applicable to legacy systems as an attachable module. New, more practical, applications such as trusted firmware upgrades and real-time malware detection and avoidance can be realized by enabling side-channel access with RASC.

54. RECYCLED/REMARKED DETECTION OF ANALOG/MIXED-SIGNAL ICS VIA LDO

Domenic Forte and Nima Maghari

Counterfeit electronics have been becoming more prevalent for the past two decades with analog ICs reportedly being the most often targeted. Electrical tests for counterfeit detection currently are impractical as a one-size-fits-all solution since there are so many different types of parts. In this project, we are studying the effects of aging on low dropout regulators (LDOs), a popular element that provides clean and stable power supply for most analog/mixed-signal and even digital chips. In general, LDOs consists of an error amplifier with a band-gap reference, and a PMOS/NMOS pass transistor feeding the error amplifier through a resistive feedback loop. Bias Temperature Instability (BTI) and Hot Carrier Injection (HCI) effects on the pass transistor and error amplifier can alter the LDO behavior as the chip is used. For a NMOS pass transistor, it will face PBTI and HCI whereas for a PMOS pass transistor there will be NBTI aging. In our initial experiments, we've found that by sweeping frequencies and measuring the power supply rejection ratio (PSRR), there is noticeable difference between used and aged LDOs, which may be useful in detecting recycled AMS chips.

55. EM SIDE-CHANNEL BASED HARDWARE SECURITY ANALYSIS

Yier Jin, Farimah Farahmandi, and Mark Tehranipoor

Side-channel information is collected from the physical implementation of a circuits, and side-channel information can be used to break into the system, obtain secret information, etc. Typically, timing information, power consumption, temperature tracking, electromagnetic leaks or even sound scan can provide an extra source of information of the circuit. While on other aspects, side-channel information is utilized by Trojans to leak specific data out of the circuit or is used as a source of fault attack. We are currently working on EM side-channel information detection and vulnerability analysis. • Establish a more precise multi parameter side channel collection system;

1. Analysis the relationship between different side channels;
2. Utilize the side-channel methods for integrated circuit security analysis;
3. Find design flaws through side-channel analysis.

56. FORMAL SECURITY VALIDATION ON RTL DESIGNS

Yier Jin

In this project, we developed a formal HDL within the Coq framework. Leveraging this formal HDL, we can either convert existing RTL code from VHDL/Verilog to formal HDL or build designs directly through the developed formal HDL. Security properties can be embedded into the design natively so that the constructed hardware designs can be formally verified to follow specified security properties. Continuing research tasks along this direction are listed as follows.

· EDA tools development. Current EDA tools do not support formal HDL. Therefore, new EDA tools and toolset are required before the formal HDL can be widely adopted in industrial designs.

· Security property. Security properties will eventually decide the security levels of the underlying designs. Upon this request, a security property library will facilitate the whole formal HDL development process.

57. HARDWARE SUPPORTED VIRTUAL MACHINE SECURITY ANALYSIS IN CLOUD ENVIRONMENT

Yier Jin

The virtualized infrastructure of cloud computing enables many mutually distrusting users to be co-hosted on the same physical hardware. As such, it is imperative that the virtual machine manager (VMM) securely isolate users from one another. Recent research on side-channel attacks have shown, despite best efforts, that the isolation and compartment guarantees offered by current VMMs are violable. These attacks are increasingly relevant because the cloud computing market shows no signs of shrinking and, in fact, will grow exponentially as Fog computing matures alongside IoT. Therefore, we aim to strengthen the security of hypervisors and VMMs against side-channel attacks by:

· Stress-testing current VMM solutions against known and new side-channels and developing common security criteria for virtualization framework assessment;

· Offering a hardened VMM implementation on Intel based cloud computing system providing process isolation and compartment against side-channel attacks.

58. IOT SECURITY VULNERABILITY DATABASE DEVELOPMENT

Yier Jin

The majority of existing research activities have addressed the IoT security mostly from a network perspective. This strategy attempts to protect the devices from a diverse set of attacks at the network level by ignoring cross-layer and hardware-layer attacks. Considering the limitations of single-layer solutions, we promote the cross-layer approach, for the first time, combining existing solutions in various layers for IoT security assessment. There is an urgent need to develop an automated IoT security assessment framework helping researchers and industrial entities across many domains (smart home, smart cities, etc.) to thoroughly evaluate the IoT protection mechanisms in order to understand the security issues and judiciously trade-off among security levels, performance overhead, and development cost. We are developing an online IoT security vulnerability database which will include all known and emerging security vulnerabilities in IoT devices. Both industrial practices and academic achievements will be integrated in constructing this database since we have been working on IoT security analysis for many years and have achieved very successful collaborations in hardware security areas. Supported by this database, a novel server-client infrastructure, called IoT-SAT, will be established to perform automatic assessment of IoT security and trust remotely for any given device.

59. LOGIC OBFUSCATION FOR IP PROTECTION

Yier Jin

Logic-locking/encryption or key-based obfuscation is based on corrupting the output of the circuit with additional key-inputs so that the circuit produces incorrect outputs without the correct secret key. IC camouflaging is a layout level technique based on creating indistinguishable layout structures for creating obscurity. These techniques can provide a layer of protection against different supply chain attacks. For instance, with logic locking, targeted malicious modification of the design is hindered through the obscurity of the obfuscated circuit and the foundry cannot overproduce the design without the correct key. In addition, both IC camouflaging and logic locking hamper IC reverse-engineering. Existing SAT attacks are oblivious to the corruptibility of the logic locking or IC camouflaging Existing SAT attacks are oblivious to the corruptibility of the logic locking or IC scheme. Therefore, we propose and study attacks that iteratively approach an approximation of the original circuit. We present a SAT based attack called AppSAT which is able to deobfuscate the high corruptibility protection in a compound scheme and is thus an approximate attack. That is, the attack reduces a compound scheme to a low corruptibility scheme which itself is a highly accurate approximation of the original circuit. In addition, we propose approximation-resilient obfuscation schemes and investigate their resiliency to different attacks.

60. DEEPSECURITY

Xiaolin (Andy) Li

Solving security problems intelligently with deep learning and protecting machine intelligence. As the key technology behind the recent renaissance of artificial intelligence, deep learning has made great successes in many areas such as computer vision, speech recognition, and machine translation. Leveraging the powerful automatic feature representation of deep learning, we design deep learning algorithms and mechanisms to help solve security problems, such as malware detection, DDoS detection, and other network/system/IoT security and privacy issues. Deep learning is also vulnerable to malicious attacks. A small perturbation of input (adversarial samples) may fool deep learning models. Attackers may also extract private models and training datasets from a black-box deep learning application. We explore the vulnerability and the countermeasures in both differential privacy and adversarial samples of deep learning.

61. BEOMSOO: HIGH PRECISION ANALOG MIXED-SIGNAL CIRCUITRY FOR COUNTERFEIT DETECTION AND SECURING SUPPLY CHAIN

Nima Maghari

A mostly passive topology which is resistant to aging and manufacturing variability by design is used to create physically unclonable functions for applications in:

1. Key generation
2. Device identification
3. Hardware monitoring

62. COST-EFFECTIVE, SCALABLE, PORTABLE ALL DIGITAL APPROACH FOR PROTECTION AGAINST IC RECYCLING AND MITIGATION OF AGING EFFECTS

Nima Maghari

Analog/Mixed-Signal ICs are among the most counterfeit, recycled and relabeled ICs. The unintended use of these counterfeit ICs in many systems can affect the accuracy, functionality or life expectancy of the system, leading to failure with possible catastrophic effects. To detect the aging and life cycle of an IC we present several key new techniques:

1. Fully digital circuits are designed to provide high fidelity aging information for detection of chip reuse and/or age calibration.
2. High density and pin-free measurement circuit drive down cost by reducing area, pin count and test overhead.

63. A FULLY-DIGITAL, UNCLONABLE SECURITY PROTOCOL FOR USE IN ANALOG/MIXED-SIGNAL SYSTEMS

Nima Maghari

As SoC grows in both market share and design complexity, more and more functions are integrated into a single silicon die. Among these, various functions are often implemented for securing the supply chain such as key generation and identification and recycling/aging/counterfeit detection. The problem arises in design cycle of these functions since most of these are either analog or mixed-signal in nature. Here, we propose a fully digital and synthesizable approach to implement all of these functions using only digital standard cells. This approach has many benefits such

1. Fast time-to-market
2. Reduced design overhead
3. Reduced circuit complexity
4. Minimized chip area
5. Maintaining excellent robustness and reliability

6. Optimized for yield and manufacturing

64. HIGH PRECISION ANALOG MIXED-SIGNAL CIRCUITRY FOR COUNTERFEIT DETECTION AND SECURING SUPPLY CHAIN

Nima Maghari

The wave of IoT has taken consumers and designer by storm, and hackers seem to be riding this wave successfully. The problem is rooted in the nature of the Tsunami-like movement we call the Internet of Things:

1. Companies are forced to be first to market or be swallowed by the tide
2. Designers need quick security solutions with less time and harsher constraints

This has led architectures which re-use functional blocks like memory to create integrated physical unclonable functions (PUFs) for key generation to come to favor. However, these PUFs fail to consider that IoT is not a purely hardware oriented movement. Any SoC made will have to run code, code that will be largely abstracted, simple, and repetitive in its use of the hardware. Inevitably, a memory based PUF will be worn down in a very specific pattern based on memory access, and this aging pattern will compromise the reliability of the system.

Instead, our approach is to implement a mostly passive topology which is resistant to aging and manufacturing variability by design and leveraging the state of the art in analog/mixedsignal circuitry to evaluate the output codes which can be used in

1. Key generation
2. Device identification
3. Hardware monitoring
4. Aging monitoring using NBTI and HCI

65. PCB ASSURANCE & SENSITIVITY ANALYSIS

Nima Maghari

The globalization of supply chain especially in electronics market is highly vulnerable due to lack of a trusted framework. Most of the manufactured systems are often in form of a Printed Circuit Board (PCB) which houses many active and passive components and are used in many systems including IoT devices, Smart Cars, Servers, and Industrial Controllers. In this effort, we seek to develop a multi-modal vulnerability analysis platform which discovers the most sensitive nodes of the circuit/ system. The merits of the sensitivity vectors can be defined by the designer to target each specific system. The outcome of the proposed vulnerability analysis platform outlines all sensitive nodes that needs further protection, pre and post fabrication circuit tests and imaging. As a result, our approach will drastically reduce the test cycle by zooming in to only sensitive nodes of the overall system rather than heuristic. Furthermore, detecting the sensitive circuit nodes in the design phase allows possible design correction and modification before the production of the system.

66. IC TROJAN INSERTION AND DETECTION

Nima Maghari

In this research we investigate insertion, analysis and functionalities of various hardware Trojans as well as hardware Trojan detection algorithms. The broad spectrum of hardware Trojans ranging from design for test to side channel leakage and spectra output detection allows optimizing Trojan detection algorithms in a full IC implementation test case.

67. LEVERAGING PASSIVE COMPONENTS IN SILICON TO IMPROVE SECURITY MERITS

Nima Maghari

One of the main challenges in maintaining proper security merits in IC design world is due to variations of process over temperature, voltage and life cycle. These variations will affect many security merits such as PUF reliability, T/RNG among others. In this effort, we introduce a new and systematic approach to leverage passive components in silicon to improve various functions such as PUF and key generation

68. INTELLECTUAL PROPERTY (IP) TRUST VALIDATION USING FORMAL METHODS

Prabhat Mishra

The wide usage of hardware intellectual property cores from untrusted vendors has raised security concerns for system designers. Existing solutions for functionality testing and verification do not usually consider the presence of malicious logic in hardware. Formal methods provide powerful solutions for detecting malicious behaviors in hardware. However, they suffer from scalability issues and cannot be easily used for large-scale computing systems. To alleviate the scalability challenge, we pro-pose a new integrated formal verification framework to evaluate the trust of system-on-chip (SoC) constructed from untrusted third-party hardware resources. This framework combines an automated model checker with an interactive theorem prover to reduce the time for proving the systemlevel security properties of SoCs. We have developed a scalable IP trust validation framework using an effective combination of property checking, theorem proving, SAT solving and equivalence checking.

69. SYSTEM-ON-CHIP SECURITY VALIDATION USING SIDE-CHANNEL ANALYSIS

Prabhat Mishra

Hardware Trojan detection has emerged as a critical challenge to ensure security and trustworthiness of integrated circuits. A vast majority of research efforts in this area has utilized side-channel analysis for Trojan detection. Functional test generation for logic testing is a promising alternative but it may not be helpful if a Trojan cannot be fully activated or the Trojan effect cannot be propagated to the observable outputs. Side-channel analysis, on the other hand, can achieve significantly higher detection coverage for Trojans of all types/sizes, since it does not require activation/ propagation of an unknown Trojan. However, they have often limited effectiveness due to poor detection sensitivity under large process variations and small Trojan footprint in side-channel signature. We address this critical problem through a novel side-channel-aware test generation approach, based on a concept of Multiple Excitation of Rare Switching (MERS), that can significantly increase Trojan detection sensitivity. The proposed work makes several important contributions: i) it presents in detail a scalable statistical test generation method, which can generate high-quality testset for creating high relative activity in arbitrary Trojan instances; ii) it analyzes the effectiveness of generated testset in terms of Trojan coverage; and iii) it describes two judicious reordering methods that can further tune the test set and greatly improve the side channel sensitivity. Simulation results demonstrate that the tests generated by MERS can significantly increase the Trojans sensitivity, thereby making Trojan detection effective using side-channel analysis.

70. SECURE NETWORK-ON-CHIP ARCHITECTURE

Prabhat Mishra

Network-on-Chip (NoC) is widely employed by multi-core System-on-Chip (SoC) architectures to cater to their communication requirements. The increased usage of NoC and its distributed nature across the chip has made it a focal point of potential security attacks. Denial-of-Service (DoS) is one such attack that is caused by a malicious intellectual property (IP) core flooding the network with unnecessary packets causing significant performance degradation through NoC congestion. We developed a lightweight and real-time DoS attack detection mechanism. Once a potential attack has been flagged, our approach is also capable of localizing the malicious IP using latency data gathered by NoC components. Experimental results demonstrate the effectiveness of our approach with timely attack detection and localization while incurring minor area and power overhead (less than 6% and 4%, respectively. We are also exploring how to develop lightweight encryption as well as anonymous routing in NoC-based SoCs.

71. POST-SILICON VALIDATION AND DEBUG

Prabhat Mishra

The goal of post-silicon validation is to ensure that the fabricated, pre-production silicon functions correctly while running actual applications under on-field operating conditions. Post-silicon validation is a complex activity performed under aggressive schedule, accounting for more than 50% of the overall validation cost of a modern integrated circuit. A fundamental challenge in post-silicon validation is limited observability and controllability. Design overhead considerations impose restrictions that only a few hundred among the millions of internal signals can be traced during a silicon execution. Furthermore, in order fora signal to be observed, the design must be instrumented a priori with appropriate hardware that routes the signal to an observation point. It is therefore crucial to develop techniques to identify trace signals that maximize design visibility under post-silicon observability restrictions. We have developed novel techniques to enhance the observability during post-silicon debug. We have also developed observability-aware test generation techniques. The application of machine learning techniques has been extensively explored to improve the scalability of trace signal selection techniques. Extensive experimental results exhibit significant improvement in both overall signal observability and signal selection time.

72. SYSTEM-ON-CHIP VALIDATION AND VERIFICATION

Prabhat Mishra

Description: Increasing complexity coupled with time-to-market pressure create a critical need to raise the abstraction level for System-on-Chip (SoC) designs. Functional validation is widely acknowledged as a major bottleneck due to lack of automated techniques and limited reuse of validation efforts between abstraction levels. Simulation is the most widely used form of validation using random or constrained-random tests. Directed tests are very promising for simulation since only fewer directed tests are required compared to billions of random tests to achieve a coverage goal. Currently, directed test generation is performed manually which is time-consuming and error-prone. We developed a novel top-down methodology for automatically generating directed tests from high-level specifications and reuse them across different abstraction levels. The objective is to reduce the overall functional validation effort. Our research has four major contributions: i) it proposes a method that can extract formal models from high-level SoC specifications; ii) it presents an approach that can automatically derive properties based on fault models; iii) it proposes efficient clustering, learning and decomposition techniques to reduce the directed test generation time; and iv) it provides validation refinement approaches to enable reuse of the system-level validation efforts for low-level implementation validation as well as to check the consistency between different abstraction layers. Our experimental results using both software and hardware benchmarks demonstrate that the proposed approaches can significantly reduce the overall validation effort. We have also explored SoC validation using an effective combination of formal verification and simulation-based techniques.

73. AGE-TARGETED AUTOMATED SECURITY CUEING AGAINST WEB-BASED SOCIAL ENGINEERING ATTACKS

Daniela Oliveira and Natalie Ebner

Online social engineering attacks have been often used for cybercrime activities. These attacks are low cost and complicate attack attribution. Pure technical defense solutions cannot counter them, which rely on human gullibility. Humans often engage in short-cut decision-making, which can lead to errors. Another expectation is that users should be able to understand complex security tips, which do not consider user demographics. User age has been overlooked in understanding these attacks and user behavior related to them. This project investigates the influence of user age on the type and the effectiveness of social engineering attacks through user studies involving young and older adults. In this research, participants are first monitored in their homes while using the Internet and receiving age-targeted malicious e-mails. Then, in a lab session involving benign and malicious Internet activities, the experimental group receives age-targeted cues about the attacks. Participants' visual attention is monitored with eye tracking technology. The results of these studies allow the development of a browser extension to cue users in an age-targeted fashion about risky situations online. This project represents a paradigm change: age-targeted security information reaches users at the time they need it, and not the other way around. This research will lead to widespread benefits on Internet safety for end-users, especially to the population of older adults, who will likely be a target of the next generation of social engineering attacks.

74. BLIND SPOTS - BUILDING DEVELOPER CENTRIC SECURITY THROUGH CROWDSOURCING

Daniela Oliveira

This research addresses an important gap in the area of vulnerability analysis: a lack of understanding of human factors in the decision-making processes that often leads to software vulnerabilities. The proposed research will capture developers’ blind spots through a novel methodology using puzzles and developer crowdsourcing. The contributions of this current research will be, but not limited to, the following areas:

1. Filling the knowledge gap in understanding developers’ blind spots while using

security critical APIs.

2. Providing important insights to understand developers' security perception and mental models
3. Developing developer-centric security intervention tools to detect vulnerabilities in blind spots and cue developers on-the-spot without habituation or annoyance.
4. Providing guidelines to design usable APIs which will help developers adopt security critical features without a steep learning curve and cognitive drain out.

75. COLLABORATIVE: DEVELOPER CROWDSOURCING: CAPTURING, UNDERSTANDING, AND ADDRESSING SECURITY-RELATED BLIND SPOTS IN APIS

Daniela Oliveira and Natalie Ebner

Despite an emphasis the security community places on the importance of producing secure software, the number of new security vulnerabilities in software increases every year. This research is based on the assumption that software vulnerabilities are caused by misunderstandings, or lack of knowledge, called blind spots, which the developers experience while they are building systems. When building systems, developers often focus more on functional requirements than on non-functional ones, such as security. Thus, they can make design decisions that prioritize functionality without noticing the security vulnerabilities these decisions create. Today, developers often have no access to effective software tools that highlight these vulnerabilities during development. This research identifies common developer blind spots with the goal of building and evaluating practical software tools that help prevent blind spots during development and detect vulnerabilities in deployed software. To capture developers' reasoning when faced with blind spots, and to identify common blind spot characteristics, this research converts several identified blind spots into programming puzzles, and conducts a user study with developers solving these puzzles. Statistical analysis of the developers' answers identifies common characteristics among blind spots, and the observations of developers' behaviors guide the creation of tools to automatically detect blind spots and to warn developers about them as developers experience them. The tools have two complementary goals: (1) prevent blind spots from occurring by cueing developers on-the-spot about potential blind spots as they write code, and (2) identify software vulnerabilities in existing applications by detecting code that may have been written as a result of a blind spot. This research evaluates these newly developed tools in the context of a user study with developers, producing the following outcomes: (1) understanding of blind spots in application programming interfaces (APIs), and of developers' attentional and decision processes when writing code using APIs, (2) understanding of how to notify, without habituation and annoyance, developers on-the-spot about blind spots so that relevant security information is used by developers while writing code, (3) creation of open-source, publicly available developer tools that notify developers about blind spots and facilitate detection of vulnerabilities caused by blind spots, and (4) development of guidelines for better API design to minimize blind spots by considering developers' attentional and decision processes. This research addresses an important gap in secure software development by incorporating the human factor of the development process. This is particularly crucial given our society's increasing dependence on software applications.

76. FINE-GRAINED ANALYSIS ON SOFTWARE SENILITY TOWARDS SYSTEM UNPREDICTABILITIES ATTACKS

Daniela Oliveira and Natalie Ebner,

We define software senility as the potential of performance degradation due to unpredictability from the OS and other applications running in the same environment. For both long-running and short-running type of software, senility occurs in a non-deterministic pattern and may last for very short period of time, making it hard to be reflected by coarse-grained resource measurement. This work proposes a fine-grained analysis on software performance degradation. We use metrics on scSOI - system call Sequence of Interest – to measure the system performance. The scSOIs represents a sequence of system calls with the minimum length that can implement a “function”. Various combinations and interactions of "functions" make up the whole execution of an application, and therefore scSOIs reveal the performance degradation in the testing application in detail.

77. FIRMA: PERSONALIZED, CROSS-LAYERED CONTINUOUS AUTHENTICATION

Daniela Oliveira and Natalie Ebner

The goal of this project is to build and evaluate FIRMA, a deep learning-based transparent and continuous authentication framework based on fine-grained cross-layer and psychological user profile. Leveraging previous work from our group, FIRMA works by continuously recording at the operating system level all fine-grained events related to processes and the files and network events spawned as a consequence of this process activity. These profiles are fed to a deep-learning module that can, after a training phase, accurately estimate the identity confidence level of the user of the system. This confidence level can be used by a system/security administrator to determine the level of access the user can have on system resources, based on configurable thresholds set by the organization. FIRMA's deep learning module will be able to adapt well to benign changes of profile with and without user cooperation. FIRMA can be employed not only for continuous authentication, but to aid in the detection of advanced persistent threats (APTs) and early indications of insider attacks.

78. FOCUSED SECURITY BEHAVIOR NUDGING VIA SUBLIMINAL STIMULI

Daniela Oliveira

We are exploring the use of subliminal stimuli to affect user behavior in information security-sensitive tasks such as software development. Though controversial, subliminal stimuli have been shown to affect consumer decision-making and preferences. We hypothesize that subliminal stimuli while using software development environments can facilitate the increase of security awareness among developers and lead to better security decisions during development. From another perspective, we are testing whether malware can quantifiably alter user behavior to socially-engineer malicious attacks on users and/or user systems. Along with this study, we are investigating whether or not subliminal stimuli can have an effect on habituation to security warnings. As users become accustomed to security warnings on their computer, their attention to warning content decreases, and habituated responses increase. We are testing whether a more subtle method of nudging users while making security decisions can decrease the rate of habituation.

79. MACHINE LEARNING FOR CYBER DEFENSE

Daniela Oliveira

We are currently developing our first version of usage profile base intrusion detection system. Two goals should be achieved by our system:

1. Intrusion and malware detection
2. Continuous authentication

Our system consists of a Windows driver for usage data extraction and a server performing machine learning and prediction. The system works as described below: Firstly, the Windows driver will extract 2-3 weeks of computer usage data from the user. Then, then dedicate server will learned the user's computer usage profile with these data using deep learning algorithm. After the profile is learned, clips of usage data will be extracted by the driver and sent to the server every minute to perform semi-real-time analysis to detect possible intrusion/malware and serve as continuous authentication. If any suspicious action was detected, both the current user and the administrator will be notified. The result could also be used to guide forensic analysis system like dynamic information flow tracking (DIFT) system to reduce unnecessary performance loss by switch it off at low risk situation.

80. RANSTOP: A HARDWARE-ASSISTED RUNTIME CRYPTO-RANSOMWARE DETECTION TECHNIQUE

Fahim Rahman, Mark Tehranipoor and Farimah Farahmandi

Among many prevailing malware types, crypto-ransomware poses a significant threat as it financially extorts affected users by creating a denial of access via unauthorized encryption of their documents as well as holding their documents hostage. In this project, we propose RanStop framework, which provides a hardware-assisted lightweight early detection mechanism for crypto-ransomware. It leverages the information of hardware performance counters embedded in the performance monitoring units of the modern processors to observe micro-architectural event sets. Using these micro-architectural characteristics of crypto-ransomware, RanStop relies on dynamic machine learning models to detect publically known and zero-day crypto-ransomware quickly (in a few execution cycles) instrument in the FICS facilities.

81. SECURITY ESTIMATION

Fahim Rahman and Mark Tehranipoor

Throughout the past years, hardware security threats have been greatly evolved. The increasing use of system-on-chip in the interconnected world, safety- and mission-critical systems exacerbates the scenario further by providing the attackers with more attack surface. Besides this, due to the increasing complexity of modern design, ensuring security becomes a non-trivial job. Thus, sometimes incorporating security in the design is treated as a burden that leaves the system unprotected. Considering this issue, we aim to develop a technique that can conduct a rapid estimation of security of the design along side with other metrics such as Power, Area, and performance. In this project, we will develop various metrics and automated tools to quickly estimate the security of intellectual properties against various threat models such as information leackage, side-channel vulnerabilites, fault-injection attacks, etc.

82. CENSORSHIP EVASION

Thomas Shrimpton

For most of us the internet is a source of knowledge, self-expression, and discussion. For many others around the world, however, the internet is not nearly so open. In order to subvert censorship we have used a mixture of strong traditional encryption, machine learning techniques, and Format Transforming Encryption (FTE). We have combined machine learned generative models with FTE to allows us to encrypt messages in a unique way. Our encryption scheme allows us to encrypt a file so that it appears as a legitimate image, audio sample, or text segment to a censor. Our end goal with this work is to help millions around the world freely converse, interact, and speak out free of any government or other large entities' censorship.

83. HEDGED CRYPTOGRAPHY: SALVAGING SECURITY WHEN RANDOMNESS FAILS

Thomas Shrimpton

Most cryptosystems are designed under the (often implicit) assumption that the system upon which they run will provide a source of high-quality randomness. Yet real-world systems often fail to do so: Time and time again, it has been shown that issues related to random number generators (RNGs) -- including software bugs, hardware failures, subversion of system resources, and malicious designs -- lead to breaches of the security guarantees the cryptography is meant to provide. Hedged cryptography aims to achieve some weaker (but still meaningful) security guarantee when randomness fails. In theory, there exist elegant designs of hedged cryptographic primitives, like public-key encryption. In practice, we find some unfortunate surprises. Chief among them is that the APIs presented by common software libraries do not permit the implementation of such designs. At least, not without demanding that developers cobble together low-level functionalities, and not without considerable expertise concerning security critical implementation details -- the very burdens that modern APIs try to lift from the developers' shoulders. Thus, our initial work (CRYPTO 2017) reconsiders hedged public-key encryption from the perspective of what APIs support, closing a crucial gap between theory and practice. This fresh perspective will be more broadly applied, with the explicit goals of providing practice-guided theory, and associated cryptographic primitives that are easier to "get right" in practice.

84. SECURITY OF DATA STRUCTURES

Thomas Shrimpton

Data structures are fundamental to computer science. Their design is driven largely by performance constraints, especially the time complexity of queries and the space needed to represent the data. We are often willing to trade correctness of the queries for a reduction in either time or space complexity. A classic example is Bloom filters, which support set-membership queries in constant time and using only a tiny amount of space. Bloom filters admit false-positives, meaning a query might be reported as being in the set when, in fact, it is not. Interestingly, these and other probabilistic data structures find use in security-critical applications, but their security properties are not well-understood. Our efforts aim to ameliorate this situation, by giving a provable-security treatment -- a formal and systematic development of mathematically precise syntax, security notions and security proofs -- to a broad class of modern data structures. Our initial work (ASIACRYPT 2017) begins this process by considering the correctness and privacy guarantees that are provided by a family of Bloom-filter-like structures, and by certain instantiations of dictionary data structures. These initial results open the door for a widely scoped effort to understand the security of existing data structures, as well as to build de novo structures designed with security in mind as a first-class property.

85. A PHYSICAL DESIGN FLOW AGAINST FRONT-SIDE PROBING ATTACKS BY INTERNAL SHIELDING

Mark Tehranipoor and Domenic Forte

Security-critical applications on integrated circuits (ICs) are threatened by probing attacks that extract sensitive information assisted with a focused ion beam (FIB) based circuit edit. Existing countermeasures, such as active shield, analog shield, and t-private circuit, have proven to be inefficient and provide limited resistance against probing attacks without taking FIB capabilities into consideration. In this project, we propose a FIB-aware anti-probing physical design flow, which considers FIB capabilities and utilizes computer- aided design (CAD) tools, to automatically reduce the probing attack vulnerability of an IC's security-critical nets with minimal extra design effort. The floor-planning and routing of the design are constrained by incorporating three new steps in the conventional physical design flow so that security-critical nets are protected by internal shield nets with low overhead. Results show that the proposed technique can reduce the vulnerable area exposed to probing on security-critical nets by 100% with all critical nets fully protected for both advanced encryption standard (AES) and data encryption standard (DES) modules. The timing, area, and power overheads are less than 3% per module, which would be negligible in a system-on-chip (SoC) design.

86. ACED-IT: ASSURING CONFIDENTIAL ELECTRONIC DESIGNS AGAINST INSIDER THREATS

Mark Tehranipoor, Farimah Farahmandi and Fahim Rahman

The electronics supply chain has adapted over the past few decades to become a global process. As the industry has transitioned from a vertical to a horizontal business model, the perceived vulnerability of IC design has grown dramatically. Today, powerful adversaries are attracting talented engineers to work for their companies and are offering significant payment for intellectual property. Semiconductor design IP is the defining characteristic of most companies within the supply chain, and as such, holds significant value for market competitiveness and, in some cases, national security. ACED-IT aims to provide a novel method to assure confidential electronics design against insider threats. ACED-IT leverages intricacies in the semiconductor design process to provide a more secure development environment for all entities throughout the supply chain. Here we move beyond typical threat models and assume that nearly every individual in the semiconductor design process is considered untrusted. By integrating authenticated encryption along with obfuscation and novel temporary inserted logic elements, we protect the valuable design IP from being extracted at any point in the process while providing all actors the tools to complete their roles.

87. EOFM-BASED CLOCK REVERSE ENGINEERING DEMONSTRATED ON FPGA

Mark Tehranipoor

Clock signals propagate throughout all modern digital circuitry and are critical to defining the functionality of the overall device. In this work we utilize a PHEMOS system and electro-optical frequency modulation techniques (EOFM) to detect unwanted insertions or modifications to the original circuit design. Modern ICs have well defined clock frequencies which the EOFM technique can lock onto and identify by scanning a laser over the backside silicon for frequency detection. We have demonstrated this on FPGAs and hope to expand to ASICs. FPGA's provide ample similarities to ASICs for this project as newer FPGAs restrict clock input routing to LUTs which are placed and routed during compilation and do not excite unnecessary cells.

88. FIRMWARE SECURITY: OBFUSCATION AND SYSTEM-LEVEL MUTUAL AUTHENTICATION

Mark Tehranipoor, Farimah Farahmandi and Fahim Rahman

Firmware is the brain of the embedded computing system. Hence, the security of the firmware is a big concern for developers and companies. Moreover, some highly sensitive embedded systems require to protect their systems from unauthorized access. For example, a programmable pacemaker for cardiac patients needs to run the secure and flawless firmware. If an adversary replaces the original firmware with a malware one, it may cause serious injury, even consequent death of the patients. This example raises a paramount matter that some devices should run only with a specific firmware. Therefore, in this project, we will develop a framework to establish a mutual authentication between hardware and software (firmware). We develop a system-level mutual authentication framework based on generating a system ID (SID) that binds the firmware with the hardware. The system integrator, the designer of the hardware and the firmware, obfuscates the firmware with the system ID and burns it to the program memory of the embedded system. During run-time, the processor de-obfuscates the program and executes it depending upon successful system ID verification with the secure cloud, otherwise the system stalls. We intend to design the framework with a minimum system overhead while maximizing the security so that it can be implemented for industrial applications where security is a big concern nowadays. The overall objective of the project is not only to assure the firmware be running only on the legitimate hardware by establishing the mutual authentication between hardware and software but also to secure the firmware itself from reverse engineering.

89. ARTIFICIAL INTELLIGENCE SECURITY

Mark Tehranipoor and Farimah Farahmandi

Hardware artificial intelligence (AI) accelerators are gaining importance in many applications such as autonomous driving, industrial robots, business intelligence, and cloud infrastructures due to their ability to run complex tasks effectively. While the benefits of AI accelerators in our lives are indisputable, there are various concerns regarding the security of the deployed AI accelerators. AI accelerators' novel architectures and the data processed by them, should be protected to prevent Intellectual Property (IP) piracy, as well as the violation of privacy. An adversary can perform various attacks to have a commercial gain or unauthorized access to valuable assets of AI systems such as the structure of the neural network, weights, and fine-tuned datasets. Therefore, it is crucial to evaluate the security of AI accelerators against various attacks such as IP piracy, cloning, tampering, reverse engineering, physical, and side-channel attacks. In this project, we study the assets of the existing neural networks that should be protected against different security attacks and analyze vulnerabilities that may exist in hardware implementations of AI systems to leak the assets. We also investigate the susceptibility of AI accelerators to remote attacks that target creating misclassification in those architectures. Finally, we will propose defensive strategies and countermeasures to create secure AI systems.

90. ATTACKS ON DNN HARDWARE

Mark Tehranipoor, Farimah Farahmandi and Navid Asadi

Increase in computational capabilities, and the availability of data, hardware artificial intelligence (AI) accelerators have turned into a reality. Accelerators allow inference to be performed with lower cost, latency, higher throughput, and often at lower power. This has huge implications for systems ranging from data centers to embedded microcontrollers. AI accelerators are often found in the edge devices that are used in applications such as medical, autonomous driving, security, robotics, face and voice recognition, etc. Machine learning systems are tasked with solving complex problems, and the outputs of large neural networks are often difficult-to-explain and are considered as a black-box. Therefore, the security of these AI accelerators is a huge concern. These accelerators contain the fine- tuned models, which are considered as an intellectual property (IP). Further, the pre-trained models are also vulnerable to provide additional training data information, which could be sensitive. To achieve commercial gain or unauthorized access, an adversary can perform attacks against the fine-tuned AI model (structure, weights, biases) and training data. In addition to piracy of intellectual property, attackers may seek to cause misclassification in machine learning systems. There is no comprehensive security analysis and vulnerability assessment against reverse engineering, cloning, IP piracy, side-channel, and physical attacks for AI accelerators. In this project, we evaluate the vulnerabilities existing in the ML supply chain. We also seek to identify hardware-accessible vulnerabilities in machine learning systems introduced by network optimizations like quantization and pruning, and also to explore the implications of well-understood attacks on hardware like side-channel analysis on machine learning accelerators and provide defensive countermeasure and policies.

91. AUTOMATED ASSESSMENT OF FAULT-INJECTION ATTACKS AT THE PRE-SILICON: MODELS, METRICS, AND TOOLS

Mark Tehranipoor and Farimah Farahmandi

Researchers have proposed an array of physical or design techniques to encounter fault-injection attacks. However, most of the countermeasures are expensive with large overhead, and they need extensive manual design/verification efforts, which is impractical to apply for a commercial product. One approach is to develop an assessment framework to automatically locate those most vulnerable locations in the design toward fault attacks and place emphasis on protecting these vulnerable locations so that the countermeasure would be more efficient, and the protection overhead would be reduced significantly.

However, the current electronic design automation (EDA) tools are not equipped to support automatic fault-injection attack vulnerability assessment. Hence, in order to perform a design-time evaluation of such attacks, a designer must perform a tedious manual design review, which is time-consuming and hard to guarantee the accuracy of results. Therefore, in this project, for the first time to our knowledge, we attempt to bridge the gap between the need for automated security assessment tools against fault-injection attacks and the capability of existing computer-aided design (CAD) tools commonly utilized by chip designers. We will investigate the development of an automated framework for fault- injection vulnerability assessment for designs at the higher levels of abstraction (here, RTL and gate-level) using novel models and metrics. Then, local protections will be applied to the identified vulnerable locations. At last, FPGAs will be used to evaluate and validate the efficiency of the proposed framework against fault-injection attacks.

92. BUILT-IN SELF-AUTHENTICATION (BISA) AND OBFUSCATED BISA TO COUNTER HARDWARE TROJAN INSERTION BY UNTRUSTED FOUNDRIES

Mark Tehranipoor and Domenic Forte

Most existing countermeasures against hardware Trojan insertion are limited by the need of a Trojan-free golden model; those that claim to be unbound by this requirement instead rely on models which reduces accuracy and reliability. Built-in self-authentication (BISA) prevents Trojan insertion by occupying available silicon space necessary for Trojan insertion, and therefore achieves golden-model-free deterrence of Trojan insertion. BISA cells occupying silicon space are designed to be verified through test to detect removal by untrusted foundry. Obfuscated built-in self-authentication (OBISA) further improves BISA by combining it with split manufacturing. In OBISA, connections of both BISA and functional circuitry are hidden from the untrusted foundry, therefore making attacks designed against BISA impossible; meanwhile, BISA insertion also improves security of split manufacturing by significantly increasing number of cells and connections. This is only made possible through a fast connection selection algorithm that can compute connection selections a million times faster than the best existing method, which was achieved by reduction of solution space. Our evaluation on AES and DES cores shows that OBISA can reach security levels more than two times higher, satisfy all existing layout-based security metrics, while reducing overheads from hundreds of percent to less than 13% in power, less than 5% in delay, and zero percent in area, as compared to best reported performance in existing techniques. In the future, we seek to (1) demonstrate BISA and OBISA in silicon (2) expand to protect 3D ICs against untrusted foundries, and (3) combine with camouflaging and logic locking for additional security attackers outside and inside the foundry.

93. CAD BASED SOLUTIONS TO DETECT AND STOP OPTICAL PROBING OF INTEGRATED CIRCUIT

Mark Tehranipoor and Navid Asadi

The backside of the chip is vulnerable to the attacks because the active region (transistors) of the chip can be exposed by using LASER microscopy based tools. As compared to SEM imaging the LASER microscopy do not need any kind of sample preparation (polishing) because the silicon substrate is transparent to the LASER photons. The data stored in transistors in the form of bits or any event of bit flips can be read out using the optical contactless probing techniques like EOP and EOFM under LASER based Microscopes like PHEMOS. This read out can expose the sensitive data of the chip like unencrypted data or keys to the adversary. In the project, we are developing CAD based countermeasures to detect and stop optical probing. An intelligent network of sensors can detect any optical probing and after this detection we can power down the chip, make it non-functional, zeroed the data of chip of reset the chip or any user-defined action to make an IC immune to the optical probing.

94. DESIGN OF AN ON-CHIP SECURITY ENGINE

Mark Tehranipoor and Farimah Farahmandi

Modern system-on-chip (SoC) architecture integrates many functional blocks like analog, digital, and mixed-signal IP, etc. fabricated into a single silicon substrate, thus minimizing area, power, and maximizing overall performance. Thus, secure SoC design has become imperative for its wide range of applications in critical fields. Security properties can be verified during different abstraction levels of SoC design statically using formal or another verification process, but due to its complex design, many dynamic security properties can't be checked during the design phase as it depends on run-time. Also, the final SoC is needed to protect from unauthorized access and other potential threats. In this project, we propose to design a centralized on-chip security engine that protects against diverse threats realizing system-level security policies. The security engine will enforce the security policies that prevent unauthorized access and illegal transaction into the system, ensure secure encrypted communication within the chip, protect the chip through logic obfuscation, perform secure authentication, and provisioning for crypto components. We will investigate and develop effective security policies against all potential threats and design an on-chip security engine to guarantee system-level security and trust.

95. DETECTING ZERO-DAY ATTACKS IN SOC

Mark Tehranipoor and Farimah Farahmandi

The source of security vulnerabilities are diverse, and the number of security attacks introduced hardware systems is increasing rapidly. Moreover, the lack of security experts in the design process creates weak designs with many security loopholes that can be used to launch new types of attacks against System-on-Chip (SoC) designs. For example, recently has been shown that Hardware micro architecture units such as branch predictors and speculation execution units should not leak the information of secret propagation in the design and create covert-channel attacks such as Spectre and Meltdown. In this project, we develop security rules and policies that can quickly map the zero-day attacks to the existing vulnerabilities and address them using the existing resources in the design. We will also use learning and dynamic/reconfigurable monitoring systems components to detect illegal behavior of the design and stop the potential attacks at the run-time.

96. ELECTRONIC SYSTEMS PROTECTION THROUGHOUT THE LIFECYCLE

Mark Tehranipoor and Domenic Forte

Globalization of design, fabrication, and assembly of electronic devices and systems and the rise of internet of things has raised serious concerns about the security and trustworthiness of integrated circuits (ICs) and electronic systems. In this project, we will develop a holistic end-to-end solution toward security of devices, systems, and firmware. There are a number of attacks on the microelectronic devices from the first step of the design process to end of life. Example attacks include IP piracy, IP security and trust, CAD tools induced security vulnerability, SoC security, hardware Trojan insertion, overproduction, shipping defective and out-of-spec parts, counterfeiting, reverse engineering, side channel attacks, and recycling. This project is divided into two major tasks (see Figure P6): (1) Backward Trust, where a SOC design house must ensure all IPs are secure and trustworthy. (2) Forward Trust, where all entities engaging with the SOC design house are considered untrusted and must be prevented from performing piracy and tampering. The proposed flow and set of CAD tools developed in this project will be easily extended to protect the design against side-channel attacks, fault injection, etc.

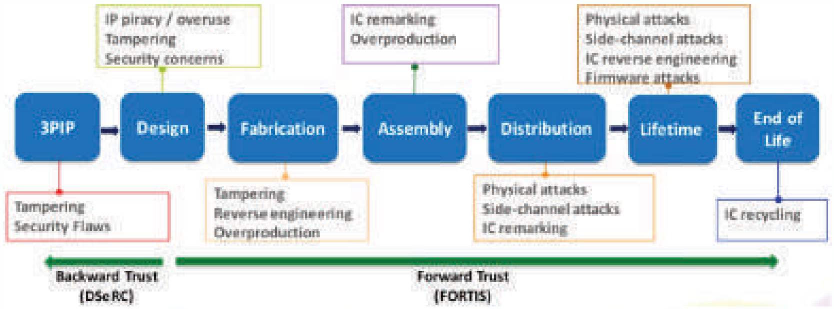


Figure P6. Microelectronics supply chain: Backward trust ensures all IPs used in SoCs are trusted and secure; Forward trust ensure that tampering and piracy is prevented throughout the supply chain. In our threat model, we assume the SoC designer in the design process is trusted. Any other entity is considered untrusted.

97. ELECTRONICS SUPPLY CHAIN INTEGRITY ENABLED BY BLOCKCHAIN

Mark Tehranipoor, Domenic Forte, Farimah Farahmandi and Fahim Rahman

In modern semiconductor business, the authenticity and integrity of the electronic components and systems are frequently questioned since the electronic supply chain is distributed all around the globe with no centralized monitoring and control offering tracking and tracing. The integrity and authenticity concerns regarding ICs and systems come from various untrusted/gray entities associated with the present-day supply chain, such as the IP owner/foundry (OCM), distributor, assembler, integrator, end user, and electronics recycler. This project analyzes the vulnerabilities and threats associated with each stage of this complex supply chain and highlights how counterfeit components can re-enter. To address the concerns of the supply chain integrity, a blockchain-based certificate authority (CA) framework is developed. Some key features of this framework are: (1) An interactive communication mechanism between all entities of the electronics supply chain and CA nodes allows tracking and tracing of electronic components and system throughout the entire life-cycle; (2) It leverages existing hardware identification modules like electronic chip ID (ECID) and chip marking, and can be used together with other existing primitives, such as physical unclonable function (PUFs); (3) The decentralized nature of the proposed framework can strongly address supply chain threats, such as recycling, remarking, cloning, and overproduction; (4) The scheme also offers compatibility for validation and maintenance for electronic components and systems. Future work for this project shall include development of communication protocols between different entities and CA network, exploring efficient data management and searching techniques, and scalable implementation considering resource constraints.

98. EMFORCED: EM-BASED FINGERPRINTING FRAMEWORK FOR REMARKED AND CLONED COUNTERFEIT IC DETECTION USING MACHINE LEARNING CLASSIFICATION

Mark Tehranipoor, Fahim Rahman, and Domenic Forte

Electronics supply chain vulnerabilities have broadened in scope over the past two decades. With nearly all IC design companies relinquishing their fabrication, packaging, and test facilities, they are forced to rely upon companies from around the world to produce their ICs. This dependence leaves the electronics supply chain open to counterfeiting activities EMFORCED, an electromagnetics-based fingerprinting framework, is designed to detect remarked and cloned counterfeit ICs. Benefiting from naturally occurring electromagnetic second-order effects to identify the IC design layout without decapsulating the chip under test. Enabling only the clock, power, and ground pins allow us to generate a design-specific fingerprint which is dependent upon the physical parameters of the chip under test.

Leveraging the emissions from the clock distribution network creates a holistic, design- level, fingerprint, including both temporal and spatial information. Statistical analysis and machine learning techniques are used to demonstrate reference-free and reference- inclusive classification methods based on EMFORCED measurements, providing various scenarios for this low-cost, fast, and zero design overhead solution.

99. EOFM-BASED CLOCK REVERSE ENGINEERING DEMONSTRATED ON FPGA

Mark Tehranipoor

Clock signals propagate throughout all modern digital circuitry and are critical to defining the functionality of the overall device. In this work we utilize a PHEMOS system and electro-optical frequency modulation techniques (EOFM) to detect unwanted insertions or modifications to the original circuit design. Modern ICs have well defined clock frequencies which the EOFM technique can lock onto and identify by scanning a laser over the backside silicon for frequency detection. We have demonstrated this on FPGAs and hope to expand to ASICs. FPGA's provide ample similarities to ASICs for this project as newer FPGAs restrict clock input routing to LUTs which are placed and routed during compilation and do not excite unnecessary cells.

100. FIRMWARE SECURITY: OBFUSCATION AND SYSTEM-LEVEL MUTUAL AUTHENTICATION

Mark Tehranipoor, Farimah Farahmandi and Fahim Rahman

Firmware is the brain of the embedded computing system. Hence, the security of the firmware is a big concern for developers and companies. Moreover, some highly sensitive embedded systems require to protect their systems from unauthorized access. For example, a programmable pacemaker for cardiac patients needs to run the secure and flawless firmware. If an adversary replaces the original firmware with a malware one, it may cause serious injury, even consequent death of the patients. This example raises a paramount matter that some devices should run only with a specific firmware. Therefore, in this project, we will develop a framework to establish a mutual authentication between hardware and software (firmware). We develop a system-level mutual authentication framework based on generating a system ID (SID) that binds the firmware with the hardware. The system integrator, the designer of the hardware and the firmware, obfuscates the firmware with the system ID and burns it to the program memory of the embedded system. During run-time, the processor de-obfuscates the program and executes it depending upon successful system ID verification with the secure cloud, otherwise the system stalls. We intend to design the framework with a minimum system overhead while maximizing the security so that it can be implemented for industrial applications where security is a big concern nowadays. The overall objective of the project is not only to assure the firmware be running only on the legitimate hardware by establishing the mutual authentication between hardware and software but also to secure the firmware itself from reverse engineering.

101 FPGA AS A SERVICE: SECURITY CHALLENGES AND OPPORTUNITIES

Mark Tehranipoor and Farimah Farahmandi

FPGAs used as hardware accelerators in the cloud domain offer unique computational service to the end-users creating a paradigm shift in the current cloud-based technological service and business trend. FPGAs pose unique threats to the cloud infrastructure due to their reconfigurability nature when compared to their counterparts (i.e., GPUs). This project aims at performing the security evaluation of user interaction and various components (FPGA, host, drivers, high-level synthesis, communication protocols, etc.) within the cloud platform and analyzing their effect on FPGA-as-a-Service overall security and privacy objectives. Security analysis of different architectural components helps in developing security metrics for FPGAs on the cloud to assist cloud-vendors for classifying threats and deploy respective countermeasures.

102. FRAMEWORK FOR AUTOMATED AND SYSTEMATIC SECURITY ASSESSMENT OF MODERN SOCS

Mark Tehranipoor and Farimah Farahmandi

A major challenge with designing secure integrated circuits (ICs) is the diversity of existing and emerging attacks, attack goals, and potential countermeasures. While security concerns in digital hardware design have become well known in recent years, a framework for comprehensive vulnerability analysis at the design stage of hardware development is still lacking. In this project, we present a new concept called Design Security Rule Check (DSeRC), to analyze vulnerabilities of a design at all levels of abstraction (register transfer level (RTL), gate-level netlist, and physical design) and assess its security at the design stage. The DSeRC framework will significantly improve the security of ICs and reduce the development time and cost by allowing the designers to identify and address security vulnerabilities at the earliest design steps.

103. HARDEN: HARDWARE-ASSISTED ML-BASED ANOMALY DETECTION FOR CYBER DEFENSE

Mark Tehranipoor and Farimah Farahmandi

In this project, we will develop a novel hardware-assisted cyber defense framework, called HARDEN, to provide complementary solutions for computing system protection. Our objective is to utilize (and propose new) hardware monitors and on-chip sensors for acquiring security critical information to intelligently assess the integrity of the system's functionality and security. Further, we will employ lightweight machine learning techniques to analyze collected hardware-based runtime signatures to detect anomaly at the architecture- and microarchitecture-levels of malicious program execution. HARDEN is reciprocal to software-only solutions to provide an integral solution to many of the cybersecurity threats, such as tampered rootkit and firmware, malware (including advanced persistent threats - APTs), ransomware, and DDoS attacks, enabling high-level assurance in modern computing systems.

Specifically, a hardware monitor can detect malicious events at runtime in a much faster and more efficient manner than a software-based technique, and can employ effective defensive mechanisms in collaboration with the operating system, for instance, terminating the exploited application, generating forensics/provenance information, and cleaning up the file system from infected files. In summary, HARDEN would be an event-driven intelligent model generation targeting threats and vulnerabilities with state-of-the- art machine learning techniques, employing hardware-level reconfigurable monitors for versatile information acquisition, and providing hardware patches for updating the ML-based detection

104. HARDWARE TROJAN DETECTION THROUGH INFORMATION FLOW SECURITY VERIFICATION

Mark Tehranipoor

Semiconductor design houses are increasingly becoming dependent on third-party vendors to procure intellectual property (IP) and meet time-to-market constraints. However, these third party IPs cannot be trusted as hardware Trojans can be maliciously inserted into them by untrusted vendors. While different approaches have been proposed to detect Trojans in third party IPs, their limitations have not been extensively studied. In this project, we analyze the limitations of the state-of-the-art Trojan detection techniques and demonstrate with experimental results how to defeat these detection mechanisms. We then propose a Trojan detection framework based on information flow security (IFS) verification.

Our framework detects a violation of IFS policies caused by Trojans without the need of white-box knowledge of the IP. We experimentally validate the efficacy of our proposed technique by accurately identifying Trojans in the trust-hub benchmarks. We also demonstrate that our technique does not share the limitations of the previously proposed Trojan detection techniques.

105. HARDWARE TROJANS IN AMS DOMAIN

Mark Tehranipoor and Farimah Farahmandi

In the AMS domain, Trojans can manifest with both analog and digital triggers as well as payloads, and it can originate from the digital part of the IC and affect the analog part or vice versa. The trigger and payload can pertain both or only the analog/digital part of the IC. Unfortunately, there has been little research efforts to detect Trojans in AMS ICs.

We plan to develop a concrete set of metrics for AMS Trojans, coupled with a new set of verification tests that fit the AMS test flow. The possible Trojan design space in AMS circuits is more complex and vaster compared to the digital counterpart due to the presence of diverse analog components, variable design parameters, and diverse possible payloads. To facilitate the security validation of AMS designs, we explore analog Trojan attack space, potential solutions, and their countermeasures. In this project, we will develop a comprehensive analog Trojan attack taxonomy, identify examples of Trojan attacks in realistic AMS designs, and develop tools for automatic generation of Trojan instances for a given AMS design. We will also create a set of metrics to localize and detect analog hardware Trojans automatically.

106. IOTIC: AN INTERNET OF THINGS INTEGRITY CHECKER

Mark M. Tehranipoor

The Internet of Things (IoT) is transforming how we live and work by increasing the connectedness of people and things on a scale that was once unimaginable. In addition to increased communication efficiency between connected objects, the IoT also brings new security and privacy challenges. Effective measures that protect IoT endpoint devices from intrusions need to be built. Existing hardware, software, and network protection methods usually need to modify IoT device design, which exposes the IoT device to extra risks (e.g., software or hardware Trojan insertion by rogue employee in security solution vendor), increases design and fabrication cost, and cannot be applied to legacy devices. To mitigate this shortcoming, we propose an innovative architecture called boardlet that can be placed into the package of IoT device to collect analog emissions (e.g., current, electromagnetic field, etc.) for integrity checking and anomaly detection. Analog emissions collected from IoT device will be converted to digital signals, from which features will be extracted and used to build a fingerprint that identifies the operating status of IoT device. Before analog- to-digital conversion, noise filtering and signal amplification will be performed. The generated fingerprint should be sensitive to any type of firmware modification and network intrusion. Machine learning and classification algorithms (e.g., naïve Bayes, support vector machine, neural network, etc.) will be adopted to help identify the operating status of the IoT device. When the boardlet detects any anomaly, it will send an encrypted warning message to the IoT hub, which will forward this message to the owner of IoT device.

107. ISIP: A COMPREHENSIVE FRAMEWORK FOR INFORMATION SECURITY FOR INTELLECTUAL PROPERTY AND SYSTEM-ON-CHIP VERIFICATION

Mark Tehranipoor and Farimah Farahmandi

Due to increasing exploitation of IP and SoC vulnerabilities for adversarial attacks, there is an urgent need to develop an automated security assessment framework supporting researchers and engineers to thoroughly evaluate the information integrity, confidentiality, and asset protection mechanisms in order to evaluate the security issues and judiciously trade-off among security levels, performance overhead, and development cost. Further, such assessment would be done at the early stage of the design process with no change in the design process. Development of a security assessment framework with automated CAD tools and metrics, focusing at the pre-silicon stage, is, therefore, crucial to ensure IP and SoC security as it can offer scrutinizing and discovering the concealed vulnerabilities and resolving them in the pre-silicon design at a much faster and low-cost fashion than during the post-fabrication testing and debug, if any. In this project, we propose a comprehensive security verification framework called ISIP (Information Security for Intellectual Property Cores). ISIP operates on a netlist or synthetized RTL design, analyzes its security assets using information flow and identifies confidentiality and integrity flaws. ISIP attempts to develop frameworks to comprehensively address IP security concerns.

108. NEAR-FIELD EM FOR FOUNDRY OF ORIGIN IDENTIFICATION

Mark Tehranipoor

Provenance analysis can be extremely valuable when determining if an IC is a counterfeit part or not. This project aims to identify the fabrication facility, or foundry, of origin for an integrated circuit. With the globalization of the modern semiconductor supply chain, counterfeit detection is becoming essential for mission-critical systems. Enabling manufacturers to identify the foundry of origin for an IC properly would allow for the first line of defense against counterfeit parts. Several steps have been taken to work towards the goal of this project. A potential solution to this problem has been identified using multiple measurement techniques. We determined the generalizable test stimuli required for electrical device characterization. A sample design module has been created to run simulations on. Plausibility has been evaluated by running SPICE and COMSOL simulations, providing reasonable differentiation between technology nodes and the ability to measure these differences. The SCAN lab has acquired new data collection solutions to broaden the range of capable measurement scenarios. Lastly, preliminary experimentation using an FPGA enabled the collection of emulation data for proof-of-concept.

109. PCB TROJAN DETECTION AND PREVENTION

Mark Tehranipoor and Navid Asadi

The hardware security research community is well-acquainted with the threat posed by malicious modifications to integrated circuits ("hardware trojans"), but the threats posed by hardware trojan attacks on printed circuit boards (PCBs) have remained largely unexplored. A 2018 article published by Bloomberg titled "The Big Hack" represented the first report of a hardware trojan attack on PCBs, and several researchers would publish in the wake of "The Big Hack" to underscore the threat posed by security-oblivious PCB design. This project seeks to taxonomize both the elements of PCB design that create security vulnerabilities and the trojans that might exploit such vulnerabilities. The project will consider malicious modifications that range from parametric alteration of critical traces at manufacturing time to in-field addition of a malicious IC. The project will demonstrate novel trojans on PCBs and will generate tests to serve as a benchmark for other research on detection of PCB trojans.

110. PROTECTING OBFUSCATED CIRCUITS AGAINST ATTACKS THAT UTILIZE TEST INFRASTRUCTURE

Mark Tehranipoor, Farimah Farahmandi, Fahim Rahman and Domenic Forte

Logic locking has emerged as a promising solution to protect integrated circuits (ICs) against piracy and tampering. However, the security provided by existing logic locking techniques is often thwarted by Boolean satisfiability (SAT)-based oracle-guided attacks.

Criteria for successful SAT attacks on locked circuits include: (i) the circuit under attack is fully combinational, or (ii) the attacker has scan chain access. To address the threat posed by SAT-based attacks, we adopt the dynamically-obfuscated scan chain

(DOSC) architecture and illustrate its resiliency against the SAT attacks when inserted into the scan chain of an obfuscated design. We demonstrate, both mathematically and experimentally, that DOSC exponentially increases the resiliency against key extraction by SAT attack and its variants. Our results show that the mathematical estimation of attack complexity correlates to the experimental results with an accuracy of 95% or better. Along with the formal proof, we model DOSC architecture to its equivalent combinational circuit and perform SAT attack to evaluate its resiliency empirically. Our experiments demonstrate that SAT attack on DOSC-inserted ISCAS'89 and ITC'99 benchmark circuit timeout at minimal test time overhead, and less than 1% area and power overhead

111. PROTECTION AGAINST OPTICAL PROBING ATTACKS

Mark Tehranipoor and Navid Asadi

In this project, we propose innovative design and fabrication techniques to protect integrated circuits (ICs) against optical probing attacks including fault injection and electro- optical imaging. Since electronic devices are used in different applications, modern SoCs contain many different IP cores with different levels of criticality in their functionality, and that the optical probing attacks are carried out in many different ways, it does not seem possible to offer a silver bullet solution to the optical probing attacks. Here, we take advantage of flexibility in both circuit design and CMOS fabrication to introduce the best possible countermeasures with minimum overheads (timing, performance. And area). We introduce new methods based on: i) relocating transistors involved in the critical function (e.g., encryption steps in a crypto hardware) in such a way that more than one transistor becomes excited during attack, as opposed to single fault injection which is always the target by the attacker during fault injection analysis; ii) injecting random bits into the plaintext to ensure attacker is unable to differentiate between an injected fault bit and the randomly injected bit; iii) introduce extra reflection difference in electro-optical imaging using highly reflective nano-particles to dominate the critical reflective change of a transistor biased by voltage, so that the attackers will not be able to identify the information stored in the memory cells. Finally, the proposed techniques will be implemented on Xilinx/Altera FPGAs as well as on a small test chip to be fabricated at UF NRF, and the attacks will be evaluated using PHEMOS-1000

112. REVERSE ENGINEERING OF A NEURAL NETWORK CHIP

Mark Tehranipoor and Navid Asadi

The recent evolution of Hardware AI accelerators made running of complex data analytic tasks at the edge devices feasible. The AI accelerator chips can contain valuable assets, such as tuned machine learning algorithms and data sets, which should not be exposed to an unauthorized person. Since these accelerators are available in several consumer products, they can be targets of physical attacks and reverse-engineering. In this project, we will perform a comprehensive investigation of the underlying assets of existing and emerging AI modules, such as IPs, stored data, etc. We will perform security assessments of vulnerabilities occurring due to hardware implementations, design flaws, and trust backbone of the AI systems from the design and architectural standpoint, including side-channel and remote attacks. We will perform a set of invasive and semi- invasive attacks, such as photon emission analysis and reverse engineering on existing AI accelerators for asset extraction and propose defensive countermeasures and policies.

Finally, we will develop a systematic framework that will analyze the security requirements of an AI hardware and will provide security-aware designs, rules, and policies.

113. ROWHAMMER ATTACK: DESIRABLE OR UNDESIRABLE

Mark Tehranipoor

Are you being attacked? Understand the attack mechanism and use it in a constructive way. In this project, we are pursuing two scenarios. First, we want to detect the row- hammer vulnerable word-lines in the DRAM modules as fast as possible using Row- hammer attack mechanism plus heat and x-ray in order to help manufacturers to make the row-hammer resistant DRAMs in a fast and cheap way. In the other scenario, we tune the attack in a way to reverse engineer the mappings of logical to the physical address in DRAM modules. As a result, we are able to run the reliability tests, especially the data- dependent tests on DRAM modules faster and more efficiently. It also can be used by the attackers to apply the Row-hammer attack more precisely.

114. AUTOMATED POWER SIDE-CHANNEL LEAKAGE ASSESSMENT AT RTL

Mark Tehranipoor and Farimah Farahmandi

Power side-channel attacks (SCAs) have become a major concern to the security community due to their non-invasive feature, low-cost, and effectiveness in extracting secret information from the hardware implementation of crypto-algorithms. Therefore, it is imperative to evaluate if the hardware is vulnerable to SCAs during its design and validation stages. Currently, however, there is a little known effort in evaluating the vulnerability of hardware to SCAs at the early design stage. In this project, we propose, for the first time, an automated framework, named RTL-PSC, for power side-channel leakage assessment of hardware crypto designs at the register-transfer level (RTL) with built-in evaluation metrics. RTL-PSC first estimates the power profile of hardware design using functional simulation at RTL. Then it utilizes the evaluation metrics, comprising of KL divergence metric and the success rate (SR) metric based on maximum likelihood estimation to perform power side-channel leakage (PSC) vulnerability assessment at RTL. We analyze Galois-Field (GF), and Look-up Table (LUT) based AES designs using RTL-PSC and validate its effectiveness and accuracy through both gate-level simulation and FPGA results. RTL-PSC is also capable of identifying blocks*inside the design that contributes the most to the PSC vulnerability, which can be used for efficient countermeasure implementation.

115. CAD FRAMEWORK FOR POWER SIDE-CHANNEL VULNERABILITY ASSESSMENT AT GATE LEVEL

Mark Tehranipoor and Farimah Farahmandi

Power side-channel attacks (SCAs) have proven effective at extracting secret keys from hardware implementations of cryptographic algorithms. Ideally, the power side-channel leakage (PSCL) of hardware designs of a cryptographic algorithm should be evaluated as early as the pre-silicon stage (e.g., gate-level). However, there has been little effort in developing computer-aided design (CAD) tools to accomplish this. In this project, we propose an automated CAD framework called SCRIPT to evaluate information leakage through side-channel analysis. SCRIPT starts by defining the underlying properties of the hardware implementation, which can be exploited by side-channel attacks. It then utilizes information flow tracking (IFT) to identify registers that exhibit those properties and, therefore, leak information through the side-channel. Here, we develop an IFT-based side- channel vulnerability metric (SCV) that is utilized by SCRIPT for PSCL assessment. SCV is conceptually similar to the traditionally used signal-to-noise ratio (SNR) metric. However, unlike SNR, which requires thousands of traces from silicon measurements, SCRIPT utilizes formal methods to generate SCV-guided patterns/plaintexts allowing us to derive SCV using only a few patterns (ideally as low as two) at gate-level. SCV estimates PSCL vulnerability at the pre-silicon stage based on the number of plaintexts required to attain a specific SCA success rate. The integration of IFT and pattern generation makes SCRIPT efficient, accurate, and generic to be applied to any hardware design. We validate the efficacy of the SCRIPT framework by demonstrating that it can effectively and accurately determine SCA success rates for different AES designs at the pre-silicon stage. SCRIPT is orders of magnitude more efficient than traditional pre-silicon PSCL assessment (SNR- based) with an average evaluation time of 15 minutes; whereas, traditional PSCL assessment at the pre-silicon stage would require more than a month. We also analyze the PSCL characteristic of the multiplication unit of the RISC processor using SCRIPT to demonstrate SCRIPT's applicability.

116. SECURE HDL

Mark Tehranipoor

Modern integrated circuits are under various attacks and information leakage threats. A great amount of these threats can be identified, mitigated or addressed at the RTL level. Therefore, we are developing a HDL verification tool to identify as many vulnerabilities in HDL code as possible, provide effective solutions at RTL level, and extract useful information for transition to next design stage for better protection. The research plan is as follows:

1. Develop security rules taxonomy
2. Explore various security rules at RTL level
3. Develop syntax to formally define a security rule
4. Software implementation to parse HDL code and security rules
5. Software implementation to check each security rule on target HDL code
6. Software implementation to modify HDL code with solutions to vulnerabilities
7. Generate vulnerability analysis report and more secure HDL code

This tool will benefit IC testing and hardware security communities by reporting security vulnerabilities and providing possible solutions at RTL level.

117. SECURE SOFTWARE VALIDATION TOOLS

Mark Tehranipoor and Farimah Farahmandi

The goal of this project is to develop comprehensive algorithms, metrics, and tool-suite for checking and validating integrity of embedded software that comprehends and accounts for hardware-software interactions and relevant architectural features, e.g., cache timing channel. Our approach uses static program analysis and formal methods, i.e., mathematical logic to either detect targeted vulnerabilities, or provide a mathematical certification of their absence. Our specific focus is on checking potential vulnerabilities of the software against diverse security attacks, including buffer/integer/counter overflows, cache timing attacks, and fault injection. A unique feature of our approach is the use of hardware invariants as constraints in such checks. Note that because of tight interaction with hardware, many potential execution paths of the software may be disallowed; a check on the software itself as a standalone module can consequently produce a significant number of spurious failures. This effect is particularly pronounced in detection of vulnerabilities to attacks on timing or speculation. To address this problem, we will develop a methodology whereby hardware invariants are discovered through analysis of register transfer logic (RTL) description and used as constraints to focus on software integrity checks.

118. SECURE REMOTE FPGA INITIALIZATION IN AN UNTRUSTED ENVIRONMENT

Mark Tehranipoor, Farimah Farahmandi and Fahim Rahman

The bitstream inside a Field-Programmable Gate Array (FPGA) is often protected using an encryption key, acting as a root of trust and stored inside the FPGA, to defend against bitstream piracy, tampering, overproduction, and static-time reverse engineering. For cost savings and faster production, trusted system designers often rely on an untrusted system assembler to program the encryption key into the FPGA, focusing only the end-user- stage threats. However, providing the secret encryption key to an untrusted entity introduces additional threats, since access to this key can compromise the entire root of trust and breach the encrypted bitstream enabling a multitude of attacks including Trojan insertion, piracy and overproduction. To address this issue, we propose the Secure Remote FPGA Initialization (SeRFI) protocol to transmit the encryption key securely from a trusted system designer into an FPGA in physical possession of an untrusted system assembler. Our protocol eliminates direct key sharing with the untrusted system assembler as well as prevents against adversarial intention of extracting the encryption key during the programming phase where the assembler has physical access to the FPGA.

119. SPARTA: LASER PROBING APPROACH FOR TROJAN DETECTION

Mark Tehranipoor and Farimah Farahmandi

Integrated circuits fabricated at untrusted foundries are vulnerable to hardware Trojan insertion. Checking for the existence of Trojans usually requires a complex test process and design-level modifications. This results in low detection confidence and a significant increase in verification effort, making them inapplicable to complex circuits due to aggressive time-to-market constraints. On the other hand, for a high confidence detection of Trojans, an exhaustive inspection may be required using destructive reverse-engineering techniques. However, such methods are quite expensive, not applicable to all chips due to their destructive nature, and are very time-consuming. SPARTA, a non-destructive laser probing approach for Trojan detection, detects sequential hardware Trojans by comparing clock activity within the IC with the original clock tree created in the design phase. SPARTA does not need any golden samples, but rather the golden design. SPARTA is based upon creating a 2-dimensional frequency map of the backside silicon using electro-optical frequency mapping (EOFM), which extracts activity from clocked elements in the IC. The measurements are then compared with the expected sequential activity based on the clock tree identified in the IC design phase, and the differences in measured activity indicate circuit modifications and the presence of sequential hardware Trojans. SPARTA confidently identifies all additions, subtractions, or modifications to sequential elements with sub-micron spatial resolution and has been demonstrated on a 28nm device.

120. TEST-CHIP DESIGN FOR SECURITY ASSESSMENT

Domenic Forte and Mark Tehranipoor

FICS research institute and its faculties has been playing the pioneer role in hardware security and CyberSecurity domain for a long time, developing several ground-breaking security primitives and playing influential role in forwarding newer research directions. We are developing a test-chip that will implement our several in-house research projects e.g. multi-layer shield, back-side shield, anti-optical probing, EM analysis, power analysis, dynamic power analysis, side-channel attack and probing attack on logic locked design, trojan scanner etc. For this project are collaborating with musesemi.com and University of Bremen to design and fabricate the test-chip. Some of our projects going to this test-chip requires reverse engineering capability. For that we have developed our own standard-cells. Rest of the chip will use ARM cells. This chip will be fabricated in TSMC 65nm process through Musesemi MPW run.

121. UNIVERSAL SECURITY THEORY FOR EVALUATION AND DESIGN OF NANO-SCALE DEVICES AND FOR DEVELOPMENT OF INNOVATIVE SECURITY PRIMITIVES

Mark Tehranipoor and Domenic Forte

With the increase of complexity in electronic circuits and systems and rising vulnerabilities in electronic supply chain, it has become a necessity to ensure security within the hardware itself. Although research in hardware security has prevailed till date at higher levels of abstraction (e.g., circuit and architecture) based on CMOS technology, emerging nano-devices, such as phase change memory, memristors, carbon nanotubes and graphene, etc., have also shown interesting potentials to overcome existing threats by offering device-intrinsic security and trust. The main objective of this project is to leverage emerging nano-devices to offer more in security and trust applications that may not be achievable by existing CMOS technology. To achieve this, three major tasks have been undertaken. First, (task A) device characterization and statistical modeling is done to model the basic building blocks (i.e., devices) that compose the complex security primitives, e.g., PUFs, TRNGs, etc. Property identification and composition (task B) is carried out to identify the inherent security potentials of the emerging devices and build a universal composition model that corresponds the quality of the designed security primitives and resiliency against prevailing hardware attacks (evaluated by security metrics). Finally, we do evaluation and redesign (if necessary) based on the developed models, designs and collected data.

122. UPGRADE: AUTOMATED SYSTEM FOR UPGRADING LEGACY ELECTRONICS SYSTEMS

Mark Tehranipoor, Nima Maghari, Domenic Forte, and Prabhat Mishra

Legacy electronic systems are expected to remain an integral part of many organizations that develop and manage critical infrastructures for the foreseeable future. The cost of designing or replacing these complex systems is often extremely high and it involves significant engineering resources that such efforts become infeasible. However, the prevalence of legacy electronic systems raises serious concerns whenever legacy software or hardware components need to be replaced. Reliance on legacy systems is problematic due to the difficulty of integration with newer systems, time, risk and cost associated with (obsolete) component acquisition, prevalence of counterfeit electronic components, and the inability to mitigate security vulnerabilities when they are discovered. UPGRADE's main objective is to develop methodologies to replace a legacy system with a new system that possesses the same functionality and meets the original or users' input specifications. Primary goals of this project include: (1) understanding the key challenges for upgrading a legacy system; (2) development of innovative approaches that accurately and automatically reverse engineers a legacy system's printed circuit boards (PCBs) into a schematic; (3) deriving the functionality of the legacy system that is being replaced or upgraded from the PCB and its components; UPGRADE will then implement the extracted function into an FPGA while ensuring same functionality and specification is met with rigorous test process.

123. AUTHENTICATED TELEPHONY

Patrick Traynor

Telephone networks remain of paramount importance to society since their invention 140 years ago. They are especially important for sensitive business communications (e.g., confirming large financial transactions), whistle-blowers and journalists, and as reliable fallback when other communication systems fail. Despite the critical role telephones play in the modern communication landscape, the telephony network is unable to provide basic security guarantees. We design systems and protocols to provide strong security guarantees for the modern telephony network. Our work prevents a wide range of abusive behaviors seen within the telephone network including robo-calls, telephone based scams, and Caller-ID spoofing. Our work aims at practical deployability, and seeks to provide defenses not only for providers, but also directly to targeted users.

124. CHARACTERIZING AND STRENGTHENING THE MODERN HEALTH ECOSYSTEM

Patrick Traynor

From surgical robots to servers to MRI machines, devices in a hospital network are in charge of the patient's health and their medical well-being. As such, these devices need to be constantly available for doctors and nurses to keep track of their patients. Any disruption to these systems may cause damages that range from outdated medical records to potential death. Unfortunately, recent ransomware attacks, such as WannaCry and Petya, have shown just how vulnerable a hospital network really is by denying the availability of medical records amongst other files. While anti-viruses help prevent such malice from happening, they are installed on end hosts and do not protect the network as a whole. To address this issue, we are performing a comprehensive measurement study of a real hospital network. At a high level, we look to both affirm that the security practices are good and that no questionable traffic is being detected. Even with such preventative measures, compromised devices can still be possible. As such, our research also focuses on creating defensive profiles that can identify other potentially vulnerable devices in the network in order to prevent further propagation of malicious content.

125. ENHANCING ELECTRONIC PAYMENT SECURITY

Patrick Traynor

Electronic payments are essential to our modern economy. They allow individuals and organizations to rapidly pay for goods and services without baring the significant management responsibilities of traditional currency. Credit cards and other digital payment methods are used now more than ever. Even small independently owned businesses are now able to accept a variety of electronic payment methods. These payment technologies have gained massive popularity and are responsible for a large portion of the global economy. There are millions of users that put their trust into these systems to operate correctly and securely. However, there are vulnerabilities in electronic payment methods that currently exist that can lead to compromises in bank and credit card information. Our lab works on a on a number of different research projects in the space of electronic payment security. We address security issues with credit/debit cards, online/mobile banking, and cryptocurrency. In addition to this, we also have a variety of future research ideas in the field.

126. INTERNET OF THINGS LIFECYCLE

Patrick Traynor

The emerging and increasingly popular Internet of Things (IoT) paradigm promises many benefits. By making data a core element of every decision-making process and providing ubiquitous sensing and actuation, IoT devices could demonstrably improve efficiency, safety and convenience of modern living. Therefore, they are expected to be deployed in virtually every corner of the economy and to permeate many aspects of everyday life: from individual households to factories, from smart wearables to vehicles.

While research efforts considered specific vulnerabilities or focused on traditional issues (e.g., key management), proposed research takes into account the unique context of IoT systems, starting with initial deployment (birth), continuing through their normal operation (life) and lasting until re-purposing, caused by, e.g., ownership change, or disposal. This is significantly more difficult than in a traditional computing setting, since many IoT devices are characterized by lack of (or primitive) user interfaces and inhibited or restricted physical accessibility.

127. PROTECTING DATA WITH MANDATORY RETENTION REQUIREMENTS

Patrick Traynor

Data breaches represent a significant threat to organizations. While the general problem of protecting data has received much attention, one large (and growing) class has not - data that must be retained due to mandatory retention laws. Such data is often of little use to an organization, is rarely accessed, and represents a significant potential liability, yet cannot be discarded. In the event of a data breach, conventional encryption would not be effective as the keys (or other secrets kept around) may be compromised along with the data itself. We address this problem through a new technique called Dragchute Encryption (DE), which creates a user defined time window during which data locked via this mechanism cannot be accessed by anyone. Unlike traditional encryption schemes (where key management becomes an issue), DE is constructed in a way that the unlock mechanism requires time (rather than a secret) to retrieve the encrypted data. With this system, locking is fast and provides verifiable, non-parallelizable computational protection against unlocking.

128. SECURING EMERGING DIGITAL FINANCIAL SYSTEMS

Patrick Traynor

Mobile money is the sole financial vehicle for many people in developing countries. Typically deployed by telecommunication companies, mobile money services rely on cellular networks and allow users to make financial transactions without a bank account. In many instances, mobile money is the only means of electronic exchange in many places, has helped to raise many out of poverty, has great upside here in the developed world and will soon be connected to us. Security reality is a dumpster fire, as are the prospects for user privacy. Our team not only continues to perform extensive measurement in this space, but is also helping to define the future (e.g., ITU standards). Recently, we analyzed several mobile money Android applications and their policies to assess their security and privacy practices. Surprisingly, we found that many of the mobile applications lacked proper security mechanisms and often mishandled sensitive information. In addition, nearly half of the systems assessed did not have a privacy policy at all. Sadly, those with existing policies failed to address key areas, e.g. data minimization and data retention. In the future, we will expand our research to include credit granting institutions that provide lines of credit to users across the world.

129. SECURING MACHINE LEARNING SYSTEMS

Patrick Traynor

From personal assistant systems, to speaker identification and investment models, the use of machine learning (ML) models are increasingly becoming omnipresent in our daily lives. However, ML models are inherently vulnerable to a wide spectrum of attacks. Adversaries not only have the ability to craft inputs to evade detection in classification models, but also to steal entire models altogether. Thus far, the majority of proposed attacks have only focused on simple ML models like image recognition systems. We focus on extending attacks beyond this into audio. Additionally, we concentrate on investigating different mitigation techniques that can help protect ML models against theft and evasion, thereby protecting the systems on which we have come to rely.

130. DEVELOPMENT OF A BLOCKCHAIN ORIENTED SECURITY CLASS

Selcuk Uluagac and Koray Karabina

Blockchain technology provides a distributed database of digital transactions such that a transaction can be added to the chain only after it has been verified by the participants in the system. By construction, each transaction is valid, immutable, and publicly verifiable. As a result, blockchain technology creates a decentralized trusted infrastructure on which several applications can be built, including peer-to-peer electronic cash systems and smart contracts. This breakthrough innovative approach has been rapidly adopted since 2008 with increasing rate of popularity. Blockchain technology promises to be a fundamental technology in distributed systems and their security, including IoT, Smart City, and Supply Chain management. On the other hand, in-depth understanding of this technology is rather limited in our society, and there is a need to increase educational opportunities at the college level. Therefore, in this project, the PIs develop a novel hands- on upper undergraduate level course on the blockchain technology. The proposed course will include learning modules (LMs) with hands-on programming component, and with a focus on real-life applications.

131. DEVELOPMENT OF A HANDS-ON SECURITY CLASS FOR INTERNET OF THINGS

Selcuk Uluagac and Kemal Akkaya

Our daily lives include myriads of robustly networked intelligent IoT devices such as heads-up displays, bio-engineered systems, intelligent sensors, and autonomous systems. Unfortunately, these devices are under the constant threat of an increasing number of cyber attacks. IoT applications connected to the Internet from homes, schools, government agencies, nuclear stations, and private companies face millions of hacking attempts daily.

Given the increasingly critical nature of the cyberspace of these IoT devices, it is imperative that they are secured. This unfortunate situation necessitates the teaching and better educating of tomorrow’s cyber workforce in terms of security practices for the IoT realm.

Unfortunately, such educational and training opportunities at the undergraduate level are very limited. Therefore, in this project, we develop a novel hands-on upper undergraduate level security class for IoT. The proposed class will include learning modules (LMs) with hands-on labs and application examples specifically focusing on IoT security use cases.

132. DRONE-AIDED PLATFORM FOR ENABLING NEXT GENERATION INTELLIGENT TRANSPORT SYSTEMS

Selcuk Uluagac

It is expected that drones will take a major role in the connected smart cities of the future. They will be delivering goods and merchandise, serving as mobile hot spots for broadband wireless access, and maintaining surveillance and security of smart cities.

However, pervasive use of drones for future smart cities also brings together several technical and societal concerns and challenges that needs to be addressed, including in the areas of cybersecurity, privacy, and public safety. Drones, while they can be used for the betterment of the society, can also be used by malicious entities to conduct physical and cyber attacks, and threaten the society. The goal of this project is to review various aspects of drones in future smart cities, relating to cybersecurity, privacy, and public safety. We will also design privacy-aware protocols for the drone-aided next generation intelligent transportation systems of smart cities.

133. ELECTRONIC PAYMENTS ARE ESSENTIAL TO OUR MODERN ECONOMY.

Selcuk Uluagac

Sensors (e.g., light, gyroscope, accelerometer) and sensing enabled applications on a smart device make the applications more user-friendly and efficient. However, the current permission-based sensor management systems of smart devices only focus on certain sensors and any App can get access to other sensors by just accessing the generic sensor API. In this way, attackers can exploit these sensors in numerous ways: they can extract or leak users' sensitive information, transfer malware, or record or steal sensitive information from other nearby devices. In this project, we investigate the sensory side-channel (e.g., acoustic, seismic, light, temperature) threats to CPS and IoT devices and applications and evaluate the feasibility and practicality of the attacks on real CPS and IoT equipment. The result is novel sensory side-channel-aware security tools and techniques for the CPS and IoT devices and applications. Specifically, we (1) analyze the physical characteristics of the sensory CPS/IoT side-channels to understand how the physical world impacts the cyber world of CPS and

IoT devices; (2) investigate the information leakage through the sensory side-channels on the CPS and IoT devices; (3) develop a novel IDS particularly designed to be aware of the sensory CPS and IoT side-channels.

134. IDENTIFYING COUNTERFEIT SMART GRID DEVICES: A LIGHTWEIGHT SYSTEM LEVEL FRAMEWORK

Selcuk Uluagac

The use of compromised smart grid devices throughout the smart grid communication infrastructure poses several security challenges. Consequences of propagating fake data or stealing sensitive smart grid state information via compromised devices are costly. Hence, early detection of compromised smart grid devices is critical for protecting smart grid's components and data. To address these concerns, in this project, we introduce a novel system level approach to identify compromised smart grid devices.

Specifically, our approach is a configurable framework that combines system and function call tracing techniques and statistical analysis to detect compromised smart grid devices based on their behavioral characteristics. To measure the efficacy of our framework, we work with a realistic testbed that includes both resource-limited and resource-rich compromised devices and analyze various different compromised devices in our testbed. The devices communicate via an open source version of the IEC61850 protocol suite (i.e., libiec61850).

135. AN IOT FINGERPRINTING FRAMEWORK USING INHERENT DEVICE CHARACTERISTICS

Selcuk Uluagac

The number of Internet-of-Things (IoT) devices will be thirty billion by 2020.

Nonetheless, the increasing number of interconnected IoT devices pose more threats to the security of the devices, applications, and privacy of information. Indeed, recent figures reveal that about 70 percent of total IoT devices use unencrypted network services, 90 percent of devices collect sensitive personal credentials, and 60 percent of the devices have security vulnerabilities on the user interface. As IoT devices are mostly resource- limited devices, existing security techniques may not be feasible to implement fully on such limited devices. In this work, we work on building a framework to fingerprint IoT devices to identify their device types as a complementary security measure to be used in device authentication or access control or forensics analysis. Specifically, we build a device identification framework which incorporates Machine Learning (ML) techniques with IoT packet captures. Our design combines a passive non-intrusive feature selection technique targeting different IoT protocol captures with a novel ML classifier selection algorithm. Our framework aims to enable a technology that can be used as a complementary security mechanism and a forensics tool.

136. PRIVACY-AWARE WEARABLE-ASSISTED CONTINUOUS AUTHENTICATION FRAMEWORK

Selcuk Uluagac and Kemal Akkaya

The login process for a mobile or desktop device does not guarantee that the person using it is necessarily the intended user. If one is logged in for a long period of time, the user's identity should be periodically re-verified throughout the session without impacting their experience, something that is not easily achievable with existing login and authentication systems. Hence, continuous authentication, which re-verifies the user without interrupting their browsing session, is essential. However, authentication in such settings is highly intrusive and may expose users' sensitive information to third parties. To address these concerns, this project develops a novel privacy-aware wearable-assisted continuous authentication (WACA) framework. User specific data is acquired through built- in sensors on a wearable device. The user data goes through privacy-preserving operations throughout the authentication process. This login procedure can be applied to a wide variety of existing enterprise authentication systems such as university campuses, corporate Information Technology divisions, and government agencies. Continuous authentication and digital privacy are timely and relevant topics in today's Internet-centric always-on society.

137. SECURING SENSORY SIDE-CHANNELS IN CPS AND IOT DEVICES AND APPLICATIONS

Selcuk Uluagac

Sensors (e.g., light, gyroscope, accelerometer) and sensing enabled applications on a smart device make the applications more user-friendly and efficient. However, the current permission-based sensor management systems of smart devices only focus on certain sensors and any App can get access to other sensors by just accessing the generic sensor API. In this way, attackers can exploit these sensors in numerous ways: they can extract or leak users' sensitive information, transfer malware, or record or steal sensitive information from other nearby devices. In this project, we investigate the sensory side-channel (e.g., acoustic, seismic, light, temperature) threats to CPS and IoT devices and applications and evaluate the feasibility and practicality of the attacks on real CPS and IoT equipment. The result is novel sensory side-channel-aware security tools and techniques for the CPS and IoT devices and applications. Specifically, we (1) analyze the physical characteristics of the sensory CPS/IoT side-channels to understand how the physical world impacts the cyber world of CPS and IoT devices; (2) investigate the information leakage through the sensory side-channels on the CPS and IoT devices; (3) develop a novel IDS particularly designed to be aware of the sensory CPS and IoT side-channels.

138. A SUSTAINABLE IOT SOFTWARE DEVELOPMENT FRAMEWORK FOR SCIENCE AND ENGINEERING

Selcuk Uluagac

With recent initiatives such as Cyber-Physical Systems, Internet of Things, and Planetary Skin, sensor-based applications have gained new momentum in the research community and industry beyond the realm of computer engineers and scientists. Therefore, today sensors are not only used by computer engineers and scientists, but also by ecologists for observing wildlife, geophysicists for monitoring seismic activities of volcanoes, farmers for precision agriculture, civil engineers for monitoring the health of deteriorating civil structures like highways and bridges, medical doctors and nurses for monitoring patients, and technology enthusiasts to develop applications. This diverse group of engineers and scientists utilizes visualization, simulation, and programming tools to build their wireless sensor applications. Nonetheless, these tools are designed as separate standalone applications, which force science and engineering researchers to utilize multiple tools. This situation often creates confusion and hampers the development and data collection experience. To avoid the complexity of using multiple tools and to make sensor application and protocol development more accessible, a new extensible, scalable, and open-source sensor software development framework called PROVIZ is developed in this project.

139. AUTOMATIC AUTHOR ATTRIBUTION VIA STYLOMETRY

Damon L. Woodard

It is estimated at least 80% percent of the internet is text. An initial step in combating malicious cyber activity (cyber bullying, terrorist plot planning, fake news, etc.) is to establish the authorship of the communication. Authorship attribution, or author recognition, has yet to establish state-of-the-art performance under demanding circumstances. In an ideal scenario, authorship attribution is a considerably easier problem when the set of candidate authors is small, and each author has training samples of at least 1,000 words.

However, online media and communication produce data that far exceed these constraints. One method to determine authorship is the use of stylometry and machine learning.

Stylometry is defined as the application of linguistic style to attribute authorship to an anonymous text. This project investigates and seeks to overcome the challenges of small text samples drawn from a large candidate author set. Project efforts include the extraction of the most useful properties of current state-of-the-art algorithms for application to more challenging scenarios and the application of stylometric techniques to determine what exactly best constitutes authorial style. A future direction for this work is the use of generative models from which text samples can be generated to mimic the writing style of a given author in order to allow for author obfuscation for privacy based applications.

140. A FORMAL APPROACH TO DECEPTION

Tuba Yavuz

We use formal methods to improve deception as a defense mechanism. By formally specifying generic attack tactics and the protocols used for communicating with the peripherals such as USB and BLE protocols, we empower the host with prediction capabilities. The host creates cognitive biases to mislead the peripherals to gain time and improve its accuracy of detection of malicious behavior.

141. HARDWARE/SOFTWARE CO-VERIFICATION FOR SECURITY

Tuba Yavuz

Hardware solutions for security that involve the system software such as Intel SGX requires the interaction between the software and the hardware. We automatically extract models of the system software using programming model guided static analysis and combine it with a model of the hardware to check for security properties using model checking.

The number of Internet-of-Things (IoT) devices will be thirty billion by 2020.

Nonetheless, the increasing number of interconnected IoT devices pose more threats to the security of the devices, applications, and privacy of information. Indeed, recent figures reveal that about 70 percent of total IoT devices use unencrypted network services, 90 percent of devices collect sensitive personal credentials, and 60 percent of the devices have security vulnerabilities on the user interface. As IoT devices are mostly resource- limited devices, existing security techniques may not be feasible to implement fully on such limited devices. In this work, we work on building a framework to fingerprint IoT devices to identify their device types as a complementary security measure to be used in device authentication or access control or forensics analysis. Specifically, we build a device identification framework which incorporates Machine Learning (ML) techniques with IoT packet captures. Our design combines a passive non-intrusive feature selection technique targeting different IoT protocol captures with a novel ML classifier selection algorithm. Our framework aims to enable a technology that can be used as a complementary security mechanism and a forensics tool.

FACILITIES

FICS RESEARCH SCAN LAB

The FICS Research SeCurity and AssuraNce (SCAN) Lab at the University of Florida contains state-of-the-art, multi-million dollar instruments that provide the capability to perform cutting edge research on a variety of current hardware and software security issues and topics, from device-to-system assurance, security, and integrity analysis.

For any questions about SCAN Lab, please contact Lab Director Domenic Forte (dforte@ece.ufl.edu) or Assistant Lab Director Navid Asadi (nasadi@ece.ufl.edu).

PHYSICAL INSPECTION EQUIPMENT

1. Tomography- Bruker SkyScan 2211 MultiScale X-ray Nano-CT System
2. Spectroscopy and Spectrometry- (i) Magritek KEA MF 1-50 KEA2 Spectrometer: Dual Transmit Channels, Frequency Range 1 MHz – 50 MHz, Fast USB2.0 DSP module, Broadband op-amp duplexer, 1 Watt amplifier; (ii) EDAX detector mounted on SEM to perform Energy Dispersive Spectroscopy (EDS)
3. Microscopy and Circuit Edit- (i) TESCAN FERA-GM Xe Plasma FIB-SEM; (ii) TESCAN LYRA-XM Ga LMIS FIB-SEM; (iii) ZEISS ORION NanoFab He-Ne System
4. Temptronic ATS 605-S Thermostream System
5. The Summit 12000B Semi-Automated Probe Station
6. Nanoprober Imina Technologies' Nanoprobing SEM Solutions are turnkey for electrical characterization of microelectronic devices and in situ semiconductor failure analysis. Up to 8 miBot™ nanoprobers can be delivered in various configurations to adapt to customer applications requirements and equipment. The miBOT is famously easy-to-use and versatile piezo actuated micro robots that allows you to position the probes over millimeter scale samples with a resolution down to the nanometer. The 4 degrees of freedom of these nanoprobers enables the operator to easily adjust the orientation of probes in situ during experiment. Specifically designed for low current measurements, electrical characterization of nanostructures can be carried out with third party source-meter units (SMU) and signal analyzers through the shielded cabling, featuring an excellent signal-to-noise ratio. Equipped with the EBIC/EBAC, in situ preamplifiers and scan generators are compatible with the Nanoprobing Solutions to perform quantitative EBIC and low noise EBAC/RCI analyses as well.
7. PHEMOS-1000 The PHEMOS-1000 is a high-resolution optical emission microscope in near infrared (NIR) spectrum that localizes failures in semiconductor devices by detecting the light emissions caused by semiconductor device defects. Moreover, its laser scan system allows acquiring high-resolution pattern images. Different types of detectors are available for various analysis techniques, such as photon emission analysis (PEM), electro-optical probing (EOP), and OBIRCH analysis. In addition to failure analysis applications, this microscope can be deployed for reverse-engineering of integrated circuits (ICs) from the backside of the package.
8. DSLR Camera Setup The Nikon D850 digital single-lens reflex (DLSR) camera is capable of high-resolution imaging in the visual and infrared light spectra. With its 46megapixel lens, it captures small surface-mount PCB components with high

fidelity. Its lens is adaptable with various bandpass and polarizing filters, allowing us to capture board details at precise wavelengths. The D850 allows our lab to quickly visually inspect PCBs for trojan and defect detection. Moreover, its quick capture rates provide faster full-board imaging times compared to optical microscopy analysis.

ELECTRICAL TEST EQUIPMENT

1. Automatic Testing Equipment (ATE)- Verigy Ocelot ZFP, Loadboard designed for acelot ZFP, and ASIC test setup using FPGA board
2. Burn-in Test and Thermal Cycling Setup- Temptronic Bench Top Temperature Test System ATS 605 Thermostream, -20 to +225°C
3. Mixed Signal Oscilloscopes- (i) Tektronix MSO70404C, 4 GHz Mixed Signal Oscilloscope; 4 analog / 16 logic channels; (ii) Tektronix MSO2022B Mixed Signal Oscilloscope; Digital Phosphor, 200 MHz, 1 GS/s, 1M record length, 2+16–ch; (iii) Tektronix MDO3102 Mixed Domain Oscilloscope; (2) 1GHz analog channels, 10M record length, 1GHz spectrum analyzer
4. Digital Oscilloscopes- (i) Tektronix DSA8300 Digital Serial Analyzer Sampling Osciloscope; (ii) Tektronix TDS3032C DPO, 300MHZ, 2.5 GS/S, 2 CHANNEL; (iii) Tektronix TBS1202B–EDU Digital Storage Oscilloscope: 200MHz bandwidth, 2GS/s sample rate, 2 channel, 2.5K record length
5. Logic Analyzers- (i) Tektronix TLA6401 34 Channel, 25 GHz MagniVu Timing, 333 MHz State Clock, 2Mb Record Length Logic Analyzer; (ii) Tektronix TLA6404 136 Channel, 25 GHz MagniVu Timing, 333 MHz State Clock, 2Mb Record Length Logic Analyzer
6. Spectrum Analyzers- (i) Tektronix PA1000 Single–Phase Power Analyzer; (ii) Tektronix RSA5115B Real Time Signal Analyzer 1 Hz–15 GHz
7. Arbitrary Waveform Generator- Keithley 3390 50MHz Arbitrary Waveform Generator
8. Arbitrary Function Generators- (i) Tektronix AFG3101C Arbitrary Function Generator: 1Channel, 100MHz Bandwidth, 1GSa/s sampling rate, 128k points arbitrary waveform memory,14–bit vertical resolution, 10Vpp to 50ohm; (ii) Tektronix AFG3252C Arbitrary Function Generator: 2Channel, 240MHz Bandwidth, 2GMSa/s sampling rate, 128k points arbitrary waveform memory, 14–bit vertical resolution, 5Vpp to 50ohm

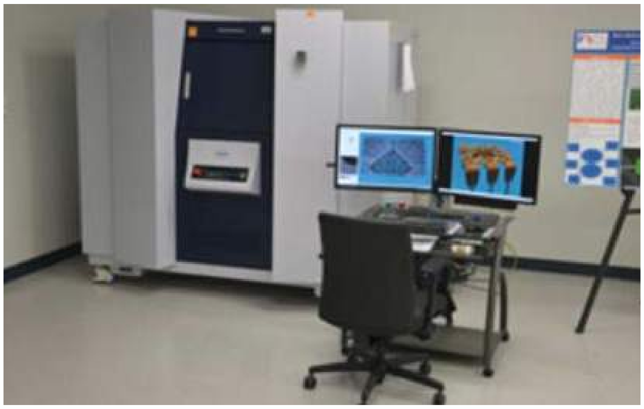
9. Power Supplies- (i) Keithley 2200–20–5 Power Supply, 20 Volts, 5 Amps DC Programmable; (ii) Keithley PWS2185 Power Supply,0–18 V, 5 Amp DC; (iii) Keithley 2231A–30–3 Manual Triple Channel DC Power Supply
10. Digital Multimeters- (i) Keithley 2100/120 6.5 Digit Dmm set to 120V; (ii) Keithley 2110–120 5.5 Digit DMM; (iii) Tektronix DMM4040 Digital Precision Multimeter, 6.5 digits 0.0035% accuracy, dual/graphic display

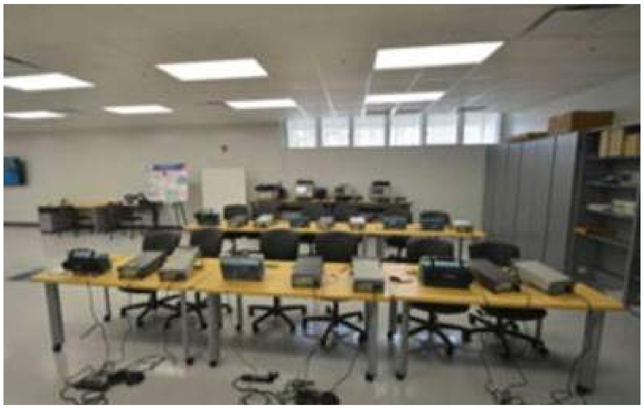
COMPUTING EQUIPMENT AND SOFTWARE

1. Workstations- 30 Dell OptiPlex workstations equipped with Windows and Linux
2. Servers- 4 Supermicro servers, each with two 10-core Xeon E5 v4 processors, 40 TB of raw storage, 12 Gbps SAS backplane, 128GB of RAM, and dual 10 Gb Ethernet.
3. CAD Tools- HSPICE, Cadence (Analog Artist, Analog Virtuoso, Diva, Pdracula, SpectreRF), Synopsys and Cadence Digital flow, ADS and HFSS and Ensemble for Electro-magnetic field simulations, Matlab

More details about FICS SCAN lab and equipment can be found at:

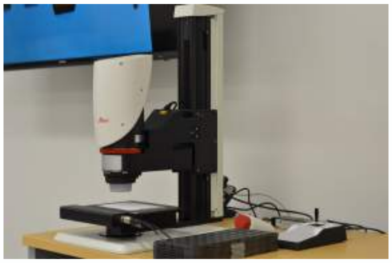
http://ficsinstitute.org/facilities/.





I: FERA-3 GMH Xe-Plasma FIB with Integrated Schottky

II: ORION NanoFab



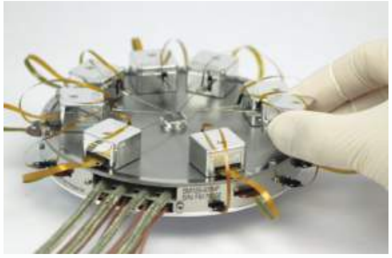
III: Leica DVM6Leica DVM6

IV: SKYSCAN 2211 MultiSclae X-ray Nano-CT System

V: LYRA-3 XMH Ga LIMIS FIB with Integrated Schottky FESEM

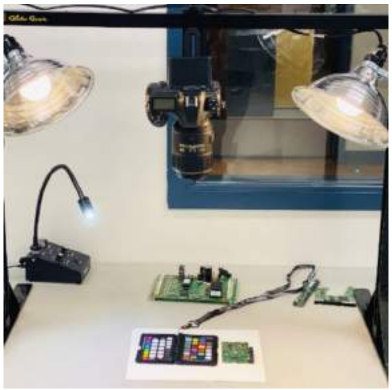
VI: Temptronic ATS 605-S Thermostream System

VII: The Summit 12000B SemiAutomated Probe Station



VIII: Nanoprober

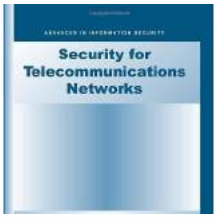
IX: PHEMOS-1000



X: DSLR Camera

FICS
Research

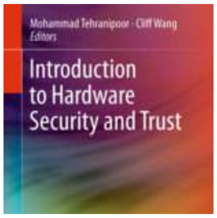
BOOKS


ADVANCES IN INFORMATION SECURITY
Security for Telecommunications Networks

Security for Telecommunications Networks (Advances in Information Security) (2008)

Traynor, P., MacDaniel, P., and La Porta, T.

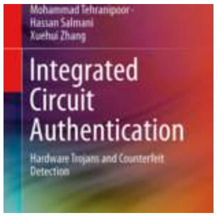
Springer publications


Mohammad Tehranipoor · Cliff Wang
Editors
Introduction to Hardware Security and Trust

Introduction to Hardware Security and Trust (2012)

Tehranipoor, M and Wang, C.

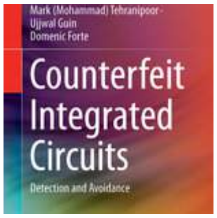
Springer publications


Mohammad Tehranipoor · Hassan Salmani · Xuehui Zhang
Integrated Circuit Authentication
Hardware Trojans and Counterfeit Detection

Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection (2014)

Tehranipoor, M and Salmani, H.

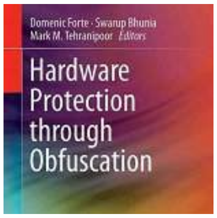
Springer publications


Mark (Mohammad) Tehranipoor · Ujjwal Guin · Domenic Forte
Counterfeit Integrated Circuits
Detection and Avoidance

Counterfeit Integrated Circuits (2015)

Tehranipoor, M., Guin U. And Forte D.

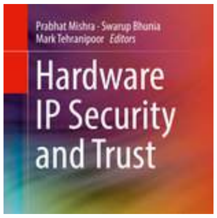
Springer publications


Domenic Forte · Swarup Bhunia · Mark M. Tehranipoor
Editors
Hardware Protection through Obfuscation

Hardware Protection through Obfuscation. (2017)

Forte, D., Bhunia, S. and Tehranipoor, M.

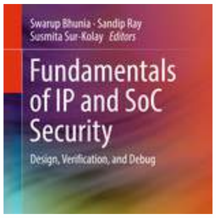
Springer Publications


Prabhat Mishra · Swarup Bhunia · Mark Tehranipoor
Editors
Hardware IP Security and Trust

Hardware IP Security and Trust (2017)

Mishra. P., Bhunia, S., and Tehranipoor, M

Springer publications


Swarup Bhunia · Sandip Ray
Susmita Sur-Kolay Editors
Fundamentals of IP and SoC Security
Design, Verification, and Debug

Fundamentals of IP and SoC Security: Design, Verification and Debug (2017)

Bhunia, S., Ray, S., and Surkolay, S.

Springer publications

Swarup Bhunia · Mark M. Tehranipoor
Editors
The Hardware Trojan War
Attacks, Myths, and Defenses

The Hardware Trojans War (2018)

Bhunia, S. and Tehranipoor, M.

Springer publications

Security Opportunities in Nano Devices and Emerging Technologies. (2018)

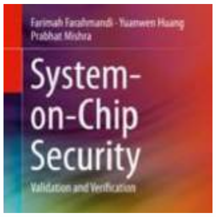
Tehranipoor, M., Forte, D, Rose, G and Bhunia S.

CRS Press

Hardware Security A Hands-on Learning Approach (2018)

Bhunia, S. and Tehranipoor, M.

Elsevier Science


Farimah Farahmandi · Yuanwen Huang
Prabhat Mishra
System-on-Chip Security
Validation and Verification

System-on-Chip Security Validation and Verification (2020)

Farahmandi, F., Huang, Y., and Mishra, P.

Elsevier Science

FACULTY BIOS

Kemal Akkaya is a full professor in the Department of Electrical and Computer Engineering at Florida International University. He received his PhD in Computer Science from University of Maryland Baltimore County in 2005 and joined the department of Computer Science at Southern Illinois University (SIU) as an assistant professor. Dr. Akkaya leads the Advanced Wireless and Security Lab (ADWISE) in the ECE Dept.

kakkaya@fiu.edu, 305-348-3017

Navid Asadizanjani is currently an Assistant Professor at the Florida Institute for Cybersecurity (FICS). He completed his Ph.D. in Mechanical Engineering from the University of Connecticut in 2014 and continued his research as post-doctoral fellow at UConn CHASE Center prior to this position. His research interests include physical assurance and inspection of integrated circuits, counterfeit detection and prevention, system and chip level reverse engineering, Antireverse engineering, etc. His results are published in several journals and conferences. He has received several awards during his Ph.D. such as ISFA best paper award and D.E. Crow innovation prize.

nasadi@ufl.edu, 352-294-1075

Vincent Bindschaedler is an Assistant Professor in the Department of Computer & Information Science & Engineering at the University of Florida. He earned his PhD in Computer Science at the University of Illinois at UrbanaChampaign in 2018. His research interests include data privacy, applied cryptography, and the intersection of machine learning with security and privacy.

vbindsch@cise.ufl.edu, 352-294-1016

Cristophe Bobda is a Professor in the Department of Electrical and Computer Engineering. He received the License in mathematics from the University of Yaounde, Cameroon, in 1992, the diploma of computer science and the Ph.D. degree (with honors) in computer science from the University of Paderborn in Germany in 1999 and 2003 respectively.

cbobda@ece.ufl.edu, 352-294-2024

Kevin Butler is an Associate Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. He is the recipient of an NSF CAREER award and has been extensively involved in technical conference organization, including chairing the ACSAC conference.

butler@ufl.edu, 352-562-0789

Shigang Chen is a Professor with Department of Computer and Information Science and Engineering at University of Florida. His research interests include computer networks, Internet security, wireless communications, and distributed computing. He published more than 190 peer-reviewed journal/conference papers. He holds University of Florida Research Foundation (UFRF) Professorship and University of Florida Term Professorship from 2017 to 2020. He is a Fellow of IEEE, an ACM Distinguished Member, and a Distinguished Lecturer of IEEE Communication Society.

sgchen@cise.ufl.edu, 352-221-9215

Natalie Ebner is currently an Associate Professor in the Department of Psychology in the College of Liberal Arts and Sciences at University of Florida (UF). She also holds an adjunct faculty position in the Department of Aging & Geriatric Research in the College of Medicine at UF and is affiliated with the Institute on Aging, the McKnight Brain Institute, and the FICS Research on campus. She obtained her Ph.D. in Psychology from the Free University of Berlin and completed post-doctoral fellowships at the Max Planck Institute for Human Development in Berlin, Germany, and at Yale University, where she worked as Associate Research Scientist before joining the faculty at UF.

natalie.ebner@ufl.edu

Yuang (Michael) Fang is a Professor in the Department of Electrical and Computer Engineering where he founded and directs the Wireless Networks Laboratory (WINET) and participates in the Wireless Information Networking Group (WING), which supports theoretical and experimental research on wireless communication systems and networks. In 2015, he was elected as an AAAS Fellow by the America Association for the Advancement of Science for his distinguished research and contributions to the field of electrical and computer engineering, particularly for wireless network design and cybersecurity.

fang@ece.ufl.edu, 352-846-3043

Farimah Farahmandi is an assistant professor in the Department of Electrical and Computer Engineering at the University of Florida. Her research has resulted in two books, seven book chapters, and several publications in premier ACM/IEEE journals and conferences. Her research has been recognized by several awards including IEEE System Validation and Debug Technology Committee Student Research Award, Gartner Group Info-Tech Scholarship, and a nomination for the Best Paper Award in ASPDAC 2017. She also has served on many technical program committees as well as organizing committees of premier ACM and IEEE conferences. Her research has been sponsored by SRC, AFRL, DARPA, and Cisco.

farimah@ufl.edu, 352 392-0910

Renato J. Figueiredo is an Associate Professor at the Department of Electrical and Computer Engineering of the University of Florida. He has co-chaired the technical programs of the ICAC-2010 and HPDC-2013 conferences. Dr. Figueiredo's research has contributed to systems that were among the first to apply resource virtualization technique in the context of Grid and cloud computing, including In-VIGO, IPOP, and Grid Appliance.

renatof@ufl.edu, 352-392-6430

Domenic Forte is an Associate Professor in the Department of Electrical and Computer Engineering. He earned a PhD in Electrical and Computer Engineering from the University of Maryland, College Park in 2013. Dr. Forte has received multiple highly sought faculty honors and distinctions including the Presidential Early Career Award for Scientists and Engineers (PECASE) in 2019, the NSF CAREER Award in 2017, the Young Investigator Award by Army Research Office in 2017, and the George Corcoran Memorial Outstanding Teaching Award in 2008. He is coauthor of one book, coeditor of two books, and has over 150 peer-reviewed publications, mostly in the field of hardware security.

dforte@ufl.edu, 352-392-1525

Juan E. Gilbert is the Andrew Banks Family Preeminence Endowed Professor and Chair of the Computer & Information Science & Engineering Department at the University of Florida where he leads the Human Experience Research Lab (HXRL). His research focuses on Human-Centered Computing (HCC) which integrates people, technology, information, policy, culture and more to address societal issues. The goal of his research is to design, implement and evaluate innovative solutions to real-world problems. He received his PhD and M.S. in Computer Science from the University of Cincinnati and his B.S. in Systems Analysis from Miami University in Ohio.

juan@ufl.edu, 352-392-1527

Yier Jin is the Endowed IoT Term Professor in the Warren B. Nelms Institute for the Connected World and also an Associate Professor in the Department of Electrical and Computer Engineering (ECE) in the University of Florida (UF). He received his PhD degree in Electrical Engineering in 2012 from Yale University after he got the B.S. and M.S. degrees in Electrical Engineering from Zhejiang University, China, in 2005 and 2007, respectively.

yier.jin@ece.ufl.edu, 352-294-0401

Nima Maghari is an Associate professor at ECE Department of University of Florida. His main area of research is analog/mixed-signal IC design and security, ranging from high performance analog-to-digital converters (ADC), digital-to-analog converter (DAC), Physical Unclonable Functions (PUF), side channel detection and aging circuitry, and other mixed-signal circuits and systems. He is in editorial board of IEEE Journal of Solid-state Circuit Letters (JSSC-L), IEEE CICC and IET Electronics Letters. He is Senior Member of IEEE.

maghari@ece.ufl.edu, 352-392-2767

Lisa McIlrath joined the Florida Institute for Cybersecurity (FICS) Research on June 1, 2019, coming from Draper Labs in Cambridge, MA, where she was a Distinguished Member of Technical Staff and Group Leader for High-Speed and Reliable Processing and Computational Electronics. Prior to Draper, Dr. McIlrath spent two years at Raytheon/BBN Technologies as a Hardware Security expert within their Cyber-Security Business Unit. Until the end of 2014, she was the President & CEO of R3Logic, Inc., a small company that she founded in 2000 and ran successfully for 14 years, raising over $12M in contracts from DARPA/DoD and other sources.

lmcilrath@ece.ufl.edu

Prabhat Mishra is a Professor in the Department of Computer and Information Science and Engineering at the University of Florida. His research focuses on hardware security and trust validation, formal verification, embedded systems and quantum computing. His research contributions have been recognized by several awards including the NSF CAREER Award, IBM Faculty Award, three best paper awards, and EDAA Outstanding Dissertation Award. He currently serves as an Associate Editor of ACM TODAES and IEEE TVLSI. Prof. Mishra is an ACM Distinguished Scientist and a Senior Member of IEEE.

prabhat@ufl.edu, 352 294 6658

Richard E. Newman is an Assistant Professor of Computer & Information Science & Engineering at the University of Florida. He has taught classes in computer and network security, cryptography, cryptographic protocols, anonymity, operating systems, computer networks, algorithms, formal languages and computation theory, computational complexity, distributed operating systems, and powerlined communications. Dr. Newman has received over $ million in grants and contracts and published over 80 technical papers. He is a member of the IEEE and IT Computer Society, and of the ACM.

nemo@cise.ufl.edu, 352-505-1579

Daniela Oliveira received her B.S. and M.S. degree in Computer Science from the Federal University of Minas Gerais in Brazi in 1999 and 2001, respectively. After working as a software engineer for three years, she started her PhD program at the Department of Computer Science at the University of California, Davis. In June 2010, she received her Ph.D. in Computer Science from the UC Davis, where she specialized in computer security and operating systems.

daniela@ece.ufl.edu, 352-392-6618

Jungmin Park is an assistant research scientist at the Florida Institute for Cybersecurity (FICS). He received his B.S. degree and M.S. in electrical engineering from Kyunghee University, Korea, in 2007, and his M.S. in computer engineering from Kyunghee University, Korea, in 2009 and Ph.D. in computer engineering from Iowa State University, Ames, IA, in 2016. He joined the FICS research as a postdoctoral fellow in 2016.

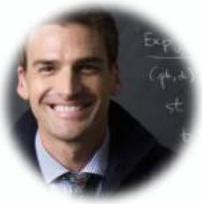
jungminpark@ufl.edu, 515-708-4711

Sandip Ray is a Professor at the Department of Electrical and Computer Engineering, University of Florida. His research involves developing trustworthy, secure, reliable computing devices and systems through a combination of architecture, synthesis, and validation technologies. Before joining University of Florida, Dr. Ray worked for several years in various capacities in industrial research labs and R&D organizations, leading research on various topics including automotive safety and security, System-on-Chip (SoC) security architecture and validation for mobile and IoT devices, postsilicon validation, and formal methods.

sandip@ece.ufl.edu, 352-392-1605

Fahim Rahman is currently a Research Assistant Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL. He received his Ph.D. in electrical and computer engineering from the University of Florida, Gainesville, in 2018. He received his BS in electrical and electronic engineering from Bangladesh University of Engineering and Technology, Bangladesh and MS in electrical and computer engineering from the University of Connecticut, USA in 2015, respectively.

fahim034@ufl.edu, 352-294-1076



Tom Shrimpton is an associate professor in the Department of Computer & Information Science & Engineering at the University of Florida. Recently, he has worked more broadly in applied cryptography. In 2009, Dr. Shrimpton was the recipient of a National Science Foundation CAREER award.

teshrim@cise.ufl.edu, 352-294-2092

Shahin Tajik is a Research Assistant Professor at the Florida Institute for Cybersecurity (FICS) Research at University of Florida. Before coming to the University of Florida, Dr. Tajik was a postdoctoral fellow at the working group SECT, a collaboration of the Technical University of Berlin and Deutsche Telekom Innovation Laboratories in Germany. He received his Ph.D. degree in Electrical Engineering in 2017 from the Technical University of Berlin.

stajik@ufl.edu, 352-294-3945

Mark M. Tehranipoor is Director of FICS Research. Currently the Intel Charles E. Young Professor in Cybersecurity at the University of Florida. Prior to joining the University of Florida, Dr. Tehranipoor served as the founding director of the Center for Hardware Assurance, Security, and Engineering (CHASE) and the Comcast Center of Excellence in Security Innovation (CSI) at the University of Connecticut. He also co-founded a new IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) the Trust-HUB forum, and the first-ever journal on hardware security, Journal of Hardware and Systems Security (HaSS).

tehranipoor@ufl.edu, 352-392-2585

Patrick Traynor is the John and Mary Lou Dasburg Preeminent Chair in Engineering. He is also an Associate professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. Dr. Traynor earned his Ph.D and M.S. in Computer Science and Engineering from Pennsylvania State University in 2008 and 2004 respectively, and his B.S. in Computer Science from University of Richmond in 2002. After promotion and tenure in the School of Computer Science at Georgia Tech, he joined the University of Florida in 2014 as part of the UF Rising Preeminence Hiring Program.

traynor@cise.ufl.edu, 352-294-2093

Selcuk Uluagac is currently an Assistant Professor in the Department of Electrical and Computer Engineering at Florida International University, where he leads the Cyber-Physical Systems Security Lab (CSL). He has served as a member of the research faculty as a Senior Research Engineer in the School of Electrical and Computer Engineering at The Georgia Institute of Technology and prior to Georgia Tech, he was a Senior Research Engineer at Symantec.

suluagac@fiu.edu, 305-348-3710

Joseph N. Wilson is an Assistant Professor in the Department of Computer and Information Science and Engineering. His primary goal is to help our next generation of graduates avoid designing and writing malware-ready programs. He is the holder of the GPEN (Penetration Tester), GXPN (Exploit Research and Advanced Penetration Tester), and GWAPT (Web Application Penetration Tester) GIAC Certifications.

jnw@cise.ufl.edu, 352-294-6678

Byron Williams is an Associate Professor in the Department of Computer and Information Science and Engineering at the University of Florida. Dr. Williams's research has focused on the intersection of software engineering and cybersecurity. Specifically, his research interests include investigating approaches to secure software development, vulnerability assessment using static and dynamic analysis, and security modeling applying statistical and machine learning techniques. Dr. Williams received his PhD from Mississippi State University.

byron@cise.ufl.edu, 352-339-0092

Damon Woodard received his Ph.D. in Computer Science and Engineering from the University of Notre Dame in 2005, his M.E. in Computer Science and Engineering from Penn State University in 1999, and his B.S. in Computer Science and Computer Information Systems from Tulane University in 1997. He is currently an Associate Professor in the Department of Electrical and Computer Engineering. He is also a founding member of the Center of Advanced Studies in Identity Science (CASIS), which is the Office of the Director National Intelligence’s (ODNI) first science and technology-based Center of Academic Excellence (CAE).

dwoodard@ufl.edu, 352-273-2130

Dapeng Oliver Wu is a Professor in the Department of Electrical & Computer Engineering and the Department of Computer and Information Science and Engineering. He obtained his Ph.D. degree in Electrical & Computer Engineering from Carnegie Mellon University, Pittsburgh, PA in 2003. He is director of UF's Multicol-12 colsm-5 col-md-3 Communications and Networking Laboratory (MCN) and is also affiliated with Wireless Information Networking Group (WING) and the Genetic Institute at UF. His most recent research projects included work on topics such as Large-Scale Real Hybrid Network Emulator and Large-Scale Power Grid Communication Networks.

wu@ece.ufl.edu, 352-392-4954

Tuba Yavuz received her Ph.D. in computer science from the Computer Science Department of University of California, Santa Barbara in 2004. She is an Assistant Professor in the Electrical and Computer Engineering (ECE) Department at the University of Florida. Her research aims to improve reliability and security of systems using formal methods and program analysis. Before joining the ECE Department, she worked as a Research Scientist at the Computer and Information Sciences and Engineering (CISE) Department at UF between 2004 and 2014.

tuba@ece.ufl.edu, 352-846-0202

SPONSORS

arm

Agilent Technologies

AFOSR
AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

AIR FORCE RESEARCH LABORATORY

ALTERA

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

ATHENA
THE ATHENA GROUP

THE ANNIE E. CASEY FOUNDATION

AVAGO
TECHNOLOGIES

BATTELLE

BMW

BRUKER

CableLabs®

CASE
WESTERN
RESERVE
EST. 1826 UNIVERSITY

CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

CISCO

COMCAST

CRA
Computing Research
Association

CYBRAICS

DARPA

DRAPER

ECI EDAPTIVE COMPUTING, INC.
Optimize • Assure • Automate • Integrate

ES&S ELECTION SYSTEMS & SOFTWARE

ellisys
Better Analysis.

EPSRC
Pioneering research and skills

everyonecounts®

DEPARTMENT OF JUSTICE • FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

Florida Center for Cybersecurity

Ford

freescale semiconductor

Graf Research

Ed

GLC²
GLC Technologies, Inc.
"a veteran-owned small business"
www.glcsquared.com

G

HARRIS®

Honeywell

intel

IBM

JUNIPER NETWORKS

Knight Foundation

LINEAR TECHNOLOGY

MEDIATEK

Mentor Graphics

Microsoft

MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE

MIT Lincoln Laboratory

NASA

NSF

NIH
National Institutes of Health

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
NOAA
U.S. DEPARTMENT OF COMMERCE

NFF
NATIONAL FOLIAGE FOUNDATION INC.

NIH National Institute on Aging

NIH National Institute on Alcohol Abuse and Alcoholism

NIST National Institute of Standards and Technology
U.S. Department of Commerce

NIH National Center for Advancing Translational Sciences

Office of Naval Research ONR Science & Technology

QUALCOMM

R'Logic

RAITH NANOFABRICATION

Rambus Cryptography Research

Raytheon

SRC Semiconductor Research Corporation

SCIENTIFIC RESEARCH NETWORK ON DECISION NEUROSCIENCE & AGING

Tektronix

TESCAN PERFORMANCE IN NANOSPACE

TEXAS INSTRUMENTS

THALES

TSYS

UNISYS

DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA

ELECTION ASSISTANCE COMMISSION UNITED STATES OF AMERICA

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA

verizon

Vetenskapsrådet

XILINX®

ZEISS

Research