Research Portfolio

The Florida Institute for Cybersecurity Research

Volume I

Gainesville, Fl
352-294-3945
http://fics.institute.ufl.edu
TABLE OF CONTENTS

About FICS Research........................................................................................................2
Technical Areas.................................................................................................................. 3
Project Titles...................................................................................................................... 4
Visual Table of Research Projects......................................................................................7
FICS Research Project Descriptions..................................................................................10
Facilities...........................................................................................................................42
Books...............................................................................................................................46
Faculty bios......................................................................................................................48
Sponsors............................................................................................................................53

Compiled by Lesly Galiana
Designed by Daniel Capecci
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.

Co-directors

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

Patrick Traynor
John & Mary Lou Dasburg Preeminent Chair in Engineering
Associate Professor
CISE Department
University of Florida

Location:
601 Gale Lemerand Drive
Materials Engineering Building (#0719)
Gainesville, FL 32603
http://fics-institute.ufl.edu
fics-research@eng.ufl.edu
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
PROJECT TITLES

P1: Machine Learning Based Hardware Trojan Detection in Third Party IPs
P2: Methodology and Tool Flow for Secure FPGA-based Systems
P3: A Wearable Carotid Ultrasound Assembly for Cardiovascular Disease Monitoring
P4: IC Electromagnetic Emission Analysis for Malware Detection
P5: A Transient Current Analysis Technique for FPGA Bitstream Reverse Engineering
P6: Electronic Systems Protection Throughout Lifecycle
P7: Hardware Trojan Detection Through Information Flow Security Verification
P8: System-on-Chip Security Architecture and CAD Framework for Hardware Patch
P9: Limit of Entropy on Chip
P10: Privacy-Preserving Multiparty Computation
P11: One-Time Programs
P12: Intel SGX-aided Solutions: FORTIS
P13: Vetting Embedded Firmware
P14: Circuit Edit Enabled Trusted Fabrication for Low Volume Products
P15: Attacks and Countermeasures for Semiconductor IP Protection
P16: Automated Non-Destructive PCB Reverse Engineering from X-Ray Computed Tomography
P17: Non-destructive Bond Pull and Ball Shear Tests for Electronics Quality Assurance and Counterfeit Detection through 3D X-ray Tomography and Finite Element Modeling
P18: Automated Reverse Engineering of Integrated Circuits
P19: Cardiovascular Biometric Authentication, Key Generation, and Presentation Attacks
P20: Metrics and Benchmarking for Logic Locking and Hardware Obfuscation
P21: Aging Resistant FPGA RO PUF
P22: Recycled/Remarked Detection of Analog/Mixed-Signal ICs via LDO
P23: Automated Counterfeit IC Defect Detection
P24: Intrinsic Memory-based Solutions Against Counterfeit ICs
P25: Obfuscation-based PCB Anti-Reverse Engineering
P26: PCB Tamper Detection
P27: A Provable-security Treatment of Counterfeiting Problems in the Electronics Supply Chain
P28: Formal Security Validation on RTL Designs
P29: Logic Obfuscation for IP Protection
P30: Hardware Supported Virtual Machine Security Analysis in Cloud Environment
P31: IoT Security Vulnerability Database Development
P32: EM Side-Channel based Hardware Security Analysis
P33: DeepSecurity
P34: Age-Targeted Automated Security Cueing Against Web-Based Social Engineering Attacks
P35: Developer Crowdsourcing: Capturing, Understanding, and Addressing Security-related Blind Spots in APIs
P36: Fine-grained Analysis on Software Senility Towards System Unpredictabilities Attacks
P37: FIRMA: Personalized, Cross-layered Continuous Authentication
P38: Focused Security Behavior Nudging via Subliminal Stimuli
P39: Machine Learning for Cyber Defense
P40: Blind Spots - Building Developer Centric Security through Crowdsourcing
P41: A Fully-Digital, Unclonable Security Protocol for Use in Analog/Mixed-Signal Systems
P42: Beomsoo: High Precision Analog Mixed-Signal Circuitry for Counterfeit Detection and Securing Supply Chain
P43: Cost Effective, Scalable, Portable All Digital Approach for Protection Against IC Recycling and Mitigation of Aging Effects
P44: Censorship Evasion
P45: Hedged Cryptography: Salvaging Security When Randomness Fails
P46: Security of Data Structures
P47: Near-Field EM for Foundry of Origin Identification
P49: Anti-probing Chip and System Design and Automated Assessment Technologies
P50: Secure HDL
P51: FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Today’s Complex Supply Chain
P52: IoTIC: An Internet of Things Integrity Checker
P53: Internet of Things Lifecycle
P54: Authenticated Telephony
P55: UPGRADE: Automated System for Upgrading Legacy Electronics Systems
P56: Securing Machine Learning Systems
P57: Securing Emerging Digital Financial Systems
P58: Protecting Data with Mandatory Retention Requirements
P59: Characterizing and Strengthening the Modern Health Ecosystem
P60: Enhancing Electronic Payment Security
P61: Electronic payments are essential to our modern economy.
P62: An IoT Fingerprinting Framework Using Inherent Device Characteristics
P63: Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework
P65: A Sustainable IoT Software Development Framework for Science and Engineering Researchers
P67: Development of A Hands-on Security Class for Internet of Things
P68: Deep Learning for Identity Sciences
P69: Automatic Author Attribution Via Stylometry
P70: A Feasibility Study of Mobile Device Usage Data for Identification and Soft Biometric Classification
P71: Hardware/Software Co-Verification for Security
P72: A Formal Approach to Deception
P73: Protection against Optical Probing Attacks
P74: HARDEN: Hardware-Assisted ML-based Anomaly Detection for Cyber Defense
P75: IPTrust: A Comprehensive Framework for IP Integrity Validation
# VISUAL TABLE OF RESEARCH

<table>
<thead>
<tr>
<th>TA1</th>
<th>TA2</th>
<th>TA3</th>
<th>TA4</th>
<th>TA5</th>
<th>TA6</th>
<th>TA7</th>
<th>TA8</th>
<th>TA9</th>
<th>TA10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.4</td>
</tr>
<tr>
<td>01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA1</td>
<td>TA2</td>
<td>TA3</td>
<td>TA4</td>
<td>TA5</td>
<td>TA6</td>
<td>TA7</td>
<td>TA8</td>
<td>TA9</td>
<td>TA10</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>P27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.1</td>
</tr>
<tr>
<td>P28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.2</td>
</tr>
<tr>
<td>P29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.3</td>
</tr>
<tr>
<td>P30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.4</td>
</tr>
<tr>
<td>P31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P37</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P39</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P42</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P44</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P47</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P52</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA1</td>
<td>TA2</td>
<td>TA3</td>
<td>TA4</td>
<td>TA5</td>
<td>TA6</td>
<td>TA7</td>
<td>TA8</td>
<td>TA9</td>
<td>TA10</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.4</td>
</tr>
<tr>
<td>P55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P56</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P57</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P58</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P61</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P62</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P66</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P67</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P68</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P70</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P72</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P73</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P74</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PROJECT DESCRIPTIONS

P1. **Machine Learning Based Hardware Trojan Detection in Third Party IPs**
Faculty: Professor Swarup Bhunia, swarup@ufl.edu; 352-392-5989
Project description: Design houses commonly integrate Intellectual Property (IP) cores acquired from third party vendors to reduce hardware design costs. While the design could be verified for specified functionality, it is extremely hard to guarantee that no hidden, and possibly malicious capability exists in form of a hardware Trojan in the untrusted third-party IP (3PIP) blocks. In this project, we introduce a systematic application of machine learning to detect malicious components inside untrusted 3PIPs. Our technique includes an automatic Trojan insertion tool that is capable of updating the Trojan database dynamically by inserting large number of Trojans of specified class. We also incorporate a systematic feature selection methodology that allows the separation of properties based on Trojan models and strengthens the detection capability.

P2. **Methodology and Tool Flow for Secure FPGA-based Systems**
Faculty: Professor Swarup Bhunia, swarup@ufl.edu; 352-392-5989
Project description: FPGAs have become very common in developing embedded Internet of Things (IoT) devices. The FPGAs that are being used in IoT products are generally low cost and operates in a resource constraint environment. Hence, high end FPGAs with built in encryption and authentication features are often not used. Besides, to evade key management issues, enhanced security features are sometime kept disabled even if available. Therefore, designs mapped onto the FPGAs become vulnerable to various attacks including cloning, reverse engineering, and tampering. To prevent these diverse attack model, we have proposed several techniques and associated CAD tools that allows a designers to accommodate these preventive solutions in legacy FPGAs. Currently, we are able to achieve strong protection against cloning and tampering using a novel bitstream obfuscation mechanism. Our solution takes advantage of “FPGA dark silicon”– unused lookup table resources to efficiently obfuscate the underlying bitstream that prevents the attacker from using the design in unauthorized manner, or tampering it.

Fig. 1: (a) Life-cycle of an FPGA based system, (b), and various forms of tampering attacks throughout the lifetime.
P3.  **A Wearable Carotid Ultrasound Assembly for Cardiovascular Disease Monitoring**  
Faculty: Professor Swarup Bhunia, swarup@ufl.edu; 352-392-5989  
Project description: The Carotid artery is one of the major vessels in human body. Located in neck, it helps supplying blood from heart to face, neck, and brain. Thus, the artery has direct and indirect association with so many diseases and pathological parameters. One of them is cardiovascular disease which is currently responsible for a major portion of all global deaths. In this project, we are trying to build a novel wearable ultrasonic imaging assembly for routine, easy-to-use, and economical monitoring of the carotid arteries. The device will monitor intima-media thickness (IMT), which is a proven clinically useful marker for diagnosis of cardiovascular disease and prediction of imminent cardiovascular events. So far, we have presented the design parameters and power requirements for all the essential hardware components of the proposed wearable imaging system and an efficient algorithm for predicting IMT anomalies from ultrasound images. Future works include building the prototype and making it applicable for some other health monitoring application too.

P4.  **IC Electromagnetic Emission Analysis for Malware Detection**  
Faculty: Professor Swarup Bhunia, swarup@ufl.edu; 352-392-5989  
Project description: Every clock-driven-IC device emits electromagnetic waves, these waves are naturally generated and cannot be controlled. The IC generates a unique pattern for every operation and it can be recorded for normal operation (golden model). Different electromagnetic signatures can be obtained by using a magnetic field probe to measure the emitted wave’s pattern. The probe can either record a pattern in time or frequency domain and both forms of the signal are used in this analysis. A change in the IC’s behavior can be reflected on the electromagnetic signature and by recording the signature of a normally operational IC any change should be noticed. The objective in this project is to record and analyze the pattern of a malware infected IC when it is in a normal operation. Different techniques can be used to identify a malicious activity when compared to the golden model. Changes in emission patterns can also be caused by IC’s age, authenticity and process variation, and all of these aspects are considered when applying this malware detection technique.

P5.  **A Transient Current Analysis Technique for FPGA Bitstream Reverse Engineering**  
Faculty: Professor Swarup Bhunia, swarup@ufl.edu; 352-392-5989  
Project description: Unlike ASICs, FPGA configuration is not physically implemented and cannot be obtained by applying invasive reverse engineering methods used in post silicon devices. The transient current analysis of an FPGA can provide an indication on how the FPGA is configured. Applying diverse or random input patterns can give unique transient current signatures that may be helpful in identifying internal signals and their transition status. Applying various DSP techniques to the transient current is the next step to extract the number and polarity of internal bit transitions. A prediction list of possible output patterns can be generated based on the identified transitions, this list will have all possible values that can generate the obtained transient current trace. A library of known FPGA configurations and functions as well as basic packages are implemented, and the input pattern used to generate the obtained transient current trace is applied through this library. All possible outputs of the library is compared to all possible
outputs generated in the prediction list. Any matches between the prediction list and the library outputs indicate the possible functions that can be the true configuration of the FPGA. Every possible function can be individually tested by repeating the same process with additional input patterns that can confirm the prediction.

P6. _Electronic Systems Protection throughout the Lifecycle_
Faculty: Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585 and Domenic Forte, dforte@ufl.edu, 352-392-1525

Project description: 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.
P7. **Hardware Trojan Detection Through Information Flow Security Verification**  
Faculty: Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, and Domenic Forte, dforte@ufl.edu, 352-392-1525  
**Project description:** Semiconductor design houses are increasingly becoming dependent on third party vendors to procure IPs 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 will develop Trojan detection framework based on information flow security (IFS) verification in system-on-chip (SoC) designs. Our framework can detect violation of IFS policies caused by Trojans without the need for white-box knowledge of the IP. Our plan is to validate the efficacy of our technique on large industry design. This framework will ensure security and trustworthiness of millions of IPs used in the market today.

P8. **System-on-Chip Security Architecture and CAD Framework for Hardware Patch**  
Faculty: Professors Swarup Bhunia, swarup@ufl.edu; 352-392-5989 and Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585  
**Project description:** System-on-Chip (SoC) security architectures targeted towards diverse applications including Internet of Things (IoT) and automotive systems enforce two critical design requirements: in-field configurability and low overhead. To address these constraints, we developed a novel, flexible, and adaptable SoC security architecture that efficiently implements diverse security policies. The architecture and associated CAD flow enable “hardware patching” i.e. a hardware security policy engine that can be seamlessly and securely upgraded in field to address unanticipated attacks or new security requirements. We implemented (1) a centralized Reconfigurable Security Policy Engine (RSPE), (2) smart security wrappers, and (3) Design-for-Debug (DfD) infrastructure interface as the building blocks of the architecture. The proposed framework provides a systematic approach to represent and synthesize diverse security policies. Through extensive analysis using representative SoC models, we show, for the first time to our knowledge, that the proposed framework provides a high level of “patchability” with minimal performance and energy costs. Future work will involve further evaluation of the architecture on industrial SoC models with test chip fabrication and explore its potentials in untrusted 3PIP verification.

P9. **Limit of Entropy on Chip**  
Faculty: Professors Swarup Bhunia, swarup@ufl.edu; 352-392-5989, and Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585  
**Project description:** In the field of computer security and cryptography, entropy is associated with the unpredictability of a source of randomness. Any source with high entropy tends to yield a uniform distribution of random values. Harvesting entropy from multifarious sources of variations and extracting the randomness is one of the most crucial aspects of cryptosystems. Due to the inadequacy of systematic approaches, however, it is challenging to explore the limit of extractable entropy originating from various sources of randomness. In this work, we explore various promising properties of contemporary devices to leverage the features and translate these to the circuit and architectural levels of abstraction. The primary goal of the study is to develop an
approach to capture the extractable random features with ease and exploit the randomness to maximize their benefits to security applications without any loss of performance of the overall system. A comprehensive understanding of device composition is required to extract the significant measures of security primitive quality metrics such as uniqueness, randomness, and most importantly, reliability. Consequently, we analyze the different architectural compositions of various devices that can lead to superior designs of hardware security primitives like PUFs, TRNGs, and Anti-Counterfeit circuitries.

P10. **Privacy-Preserving Multiparty Computation**  
**Faculty:** Professor Kevin Butler, butler@ufl.edu, 352-562-0789  
**Project description:** 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.

P11. **One-Time Programs**  
**Professor Kevin Butler, butler@ufl.edu, 352-562-0789**  
**Project description:** 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 one-timeness. 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.
P12. **Intel SGX-aided Solutions: FORTIS**  
Professor Kevin Butler, butler@ufl.edu, 352-562-0789  
**Project description:** 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.

P13. **Vetting Embedded Firmware**  
Professor Kevin Butler, butler@ufl.edu, 352-562-0789  
**Project description:** 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
P14. **Circuit Edit Enabled Trusted Fabrication for Low Volume Products**  
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525, Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, and Navid Asadi, nasadi@ufl.edu, 352-294-1075  
**Project description:** 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.

P15. **Attacks and Countermeasures for Semiconductor IP Protection**  
Professor Domenic Forte, dforte@ufl.edu, 352-392-1525, Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, Swarup Bhunia, swarup@ufl.edu, 352-392-5989  
**Project description:** 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.
P16. **Automated Non-Destructive PCB Reverse Engineering from X-Ray Computed Tomography**  
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525, Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, Navid Asadi, nasadi@ece.ufl.edu, 352-294-1075, and Damon Woodard, dwoodard@ufl.edu, 352-273-2130  
Project description: 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.

P17. **Non-destructive Bond Pull and Ball Shear Tests for Electronics Quality Assurance and Counterfeit Detection through 3D X-ray Tomography and Finite Element Modeling**  
Professors Navid Asadi, nasadi@ufl.edu, 352-294-1075 and Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585  
Project description: 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.
P18. **Automated Reverse Engineering of Integrated Circuits**  
Profs. Navid Asadi, nasadi@ufl.edu, 352-294-1075, Domenic Forte, dforte@ufl.edu, 352-392-1525, and Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585,  
**Project Description:** 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. Ultra-thinning 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 back-side ultra-thinning coupled to automated gas-assisted plasma FIB delayering.

P19. **Cardiovascular Biometric Authentication, Key Generation, and Presentation Attacks**  
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525 and Damon Woodard, dwoodard@ufl.edu, 352-273-2130  
**Project Description:** 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 PPG-based 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.
P20.  **Metrics and Benchmarking for Logic Locking and Hardware Obfuscation**  
Professor Domenic Forte, dforte@ufl.edu, 352-392-1525, Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, and Swarup Bhunia, swarup@ufl.edu, 352-392-5989  
**Project description:** 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 in-house 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.

P21.  **Aging-resistant FPGA RO PUF**  
Professor Domenic Forte, dforte@ufl.edu, 352-392-1525  
**Project description:** 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.

P22.  **Recycled/Remarked Detection of Analog/Mixed-Signal ICs via LDO**  
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525 and Nima Maghari, mahghari@ufl.edu, 352-392-2767  
**Project description:** 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.

P23. Automated Counterfeit IC Defect Detection
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525, Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, Navid Asadi, nasadi@ece.ufl.edu, 352-294-1075, and Damon Woodard, dwoodard@ufl.edu, 352-273-2130
Project description: 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.

P24. Intrinsic Memory-based Solutions Against Counterfeit ICs
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525 and Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585
Project description: 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.

**P25. Obfuscation-based PCB Anti-Reverse Engineering**  
Professor Domenic Forte, dforte@ufl.edu, 352-392-1525  
**Project description:** 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.

**P26. PCB Tamper Detection**  
Professor Domenic Forte, dforte@ufl.edu, 352-392-1525  
**Project description:** 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 model-assisted 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.
P27. A provable-security Treatment of Counterfeiting Problems in Electronics Supply Chain
Professors Domenic Forte, dforte@ufl.edu, 352-392-1525 and Thomas Shrimpton, teshrimp@cise.ufl.edu, 352-294-2092
Project description: 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.

P28. Formal Security Validation on RTL Designs
Professor Yier Jin, yier.jin@ece.ufl.edu, 352-294-0401
Project description: 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.

P29. Logic Obfuscation for IP Protection
Professor Yier Jin, yier.jin@ece.ufl.edu, 352-294-0401
Project description: 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.

P30. **Hardware Supported Virtual Machine Security Analysis in Cloud Environment**
Professor Yier Jin, yier.jin@ece.ufl.edu, 352-294-0401

Project description: 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.

P31. **IoT Security Vulnerability Database Development**
Professor Yier Jin, yier.jin@ece.ufl.edu, 352-294-0401

Project description: 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.
P32.  **EM Side-Channel Based Hardware Security Analysis**  
 **Professor Yier Jin**, yier.jin@ece.ufl.edu, 352-294-0401  
**Project description:** Side-channel information is collected from the physical implementation of a circuit, 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;  
- Analysis the relationship between different side channels;  
- Utilize the side-channel methods for integrated circuit security analysis;  
- Find design flaws through side-channel analysis.

P33.  **DeepSecurity**  
 **Professor Xiaolin (Andy) Li**, andyli@ece.ufl.edu, 352-392-2651  
**Project description:**  
**Aims:** 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.

P34.  **Age-Targeted Automated Security Cueing Against Web-Based Social Engineering Attacks**  
 **Professors Daniela Oliveira**, daniela@ece.ufl.edu, 352-392-6618 and **Natalie Ebner**, 203-691-0371, natalie.ebner@ufl.edu  
**Project description:** 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.

**P35. Collaborative: Developer Crowdsourcing: Capturing, Understanding, and Addressing Security-related Blind Spots in APIs**

Professors Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618 and Natalie Ebner, 203-691-0371, natalie.ebner@ufl.edu

**Project description:** 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.
P36. **Fine-grained Analysis on Software Senility Towards System Unpredictabilities Attacks**  
Professors Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618 and Natalie Ebner, 203-691-0371, natalie.ebner@ufl.edu  
**Project description:** 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.

P37. **FIRMA: Personalized, Cross-layered Continuous Authentication**  
Professor Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618 and Natalie Ebner, 203-691-0371, natalie.ebner@ufl.edu  
**Project description:** 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.

P38. **Focused Security Behavior Nudging via Subliminal Stimuli**  
Professor Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618  
**Project description:** 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.
P39. **Machine Learning for Cyber Defense**  
Professor Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618  
**Project description:** 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.

P40. **Blind Spots - Building Developer Centric Security through Crowdsourcing**  
Professor Daniela Oliveira, daniela@ece.ufl.edu; 352-392-6618  
**Project description:** 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.

P41. **A Fully-Digital, Unclonable Security Protocol for Use in Analog/Mixed-Signal Systems**  
Professor Nima Maghari, maghari@ece.ufl.edu, 352-392-2767  
**Project Description:** Standard digital cells are implemented to realize an on-chip cryptographic key generator, which is scalable and portable across both analog/mixed-signal (AMS) systems and fully-digital systems.  
In order to combat electronic counterfeiting, this fully-digital approach:  
- Reduces design overhead  
- Cuts circuit complexity  
- Minimizes chip area  
- Maintains excellent robustness and reliability
P42. **Beomsoo: High Precision Analog Mixed-Signal Circuitry for Counterfeit Detection and Securing Supply Chain**
Professor Nima Maghari, maghari@ece.ufl.edu, 352-392-2767
**Project Description:** A mostly passive topology which is resistant to aging and manufacturing variability by design is used to create physically unclonable functions for applications in:
- Key generation
- Device identification
- Hardware monitoring

P43. **Cost-effective, Scalable, Portable All Digital Approach for Protection Against IC Recycling and Mitigation of Aging Effects**
Professor Nima Maghari, maghari@ece.ufl.edu, 352-392-2767
**Project Description:**
- Fully digital circuits are designed to provide high fidelity aging information for detection of chip reuse and/or age calibration.
- High density and pin-free measurement circuit drive down cost by reducing area, pin count and test overhead.

P44. **Censorship Evasion**
Professor Thomas Shrimpton, teshrim@cise.ufl.edu, 352-294-2092
**Project Description:** 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.

P45. **Hedged Cryptography: Salvaging Security When Randomness Fails**
Professor Thomas Shrimpton, teshrim@cise.ufl.edu, 352-294-2092
**Project Description:** 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.

P46. **Security of Data Structures**
Professor Thomas Shrimpton, teshrim@cise.ufl.edu, 352-294-2092

**Project Description:** 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.

P.47 **Near-Field EM for Foundry of Origin Identification**
Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585 and Domenic Forte, dforte@ufl.edu, 352-392-1525

**Project description:** This project aims to identify the fabrication facility, or foundry, of an integrated circuit. With today’s globalized supply chain, security has never been more important. Enabling manufacturers to properly identify an IC’s foundry of origin would allow for a first line of defense against counterfeit parts. Progress thus far includes the following:

- Identifying a potential solution, through multiple measurement techniques, to this problem.
- Determining the test stimuli required to extract device characteristics electrically.
- Designing a sample module to run simulations on.
- Determining plausibility through SPICE and COMSOL simulations.
- Expanding our data collection abilities in our SCAN lab.
- Collecting emulated data through FPGA designs.

Our current approach to solve this problem utilizes the electromagnetic emissions of the circuit to generate a foundry specific signature. This project has potential applications in both commercial and government sectors as it attempts to address an industry-wide problem.

Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585 and Domenic Forte, dforte@ufl.edu, 352-392-1525

**Project description:** 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.

P49. **Anti-probing Chip and System Design and Automated Assessment Technologies**

Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585 and Domenic Forte, dforte@ufl.edu, 352-392-1525

**Project description:** Probing attacks against security-critical applications have become a serious concern. Under the help of modern circuit editing techniques, e.g. FIB, attackers can remove layers of material on the chip and probe sensitive information, which makes the chip with no “secrets”. Therefore, we are developing a FIB-aware CAD/EDA based solution against probing attacks that integrates into existing physical design flows. With the ever-increasing complexity of VLSI circuits, CAD/EDA tools already play a critical role in every aspect of chip design. We are expecting to achieve the following features for our solution:

- Confidentiality verification against probing
- Integrity verification against physical tampering
- Front-side and back-side protection against probing attacks
- Protection against electrical and optical probing attacks

We do believe this project will benefit financial, communication and other commercial industries by protecting integrity and confidentiality of secret data and crypto modules. It will also benefit consumers by protecting personal information and sensitive data. Military, defense industry and government will benefit from this project as well by protecting ID cards, preventing unauthorized disclosure of IP and tamper resistant hardware metering.
P50. **Secure HDL**
Professors Mark Tehranipoor, [tehranipoor@ufl.edu](mailto:tehranipoor@ufl.edu), 352-392-2585 and Swarup Bhunia, [swarup@ufl.edu](mailto:swarup@ufl.edu), 352-392-5989

**Project description:** 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:

- Develop security rules taxonomy
- Explore various security rules at RTL level
- Develop syntax to formally define a security rule
- Software implementation to parse HDL code and security rules
- Software implementation to check each security rule on target HDL code
- Software implementation to modify HDL code with solutions to vulnerabilities
- 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.

P51. **FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Today’s Complex Supply Chain**
Professors Domenic Forte, [dforte@ufl.edu](mailto:dforte@ufl.edu), 352-392-1525 and Mark Tehranipoor, [tehranipoor@ufl.edu](mailto:tehranipoor@ufl.edu), 352-392-2585

**Project description:** 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
P52. **IoTIC: An Internet of Things Integrity Checker**  
Professor Mark M. Tehranipoor, tehranipoor@ece.ufl.edu, 352-392-2585  
**Project description:** 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., naive 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.

P53. **Internet of Things Lifecycle**  
Professor, Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project Summary:** 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.

P54. **Authenticated Telephony**  
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project Description:** 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.

P55. **UPGRADE: Automated System for Upgrading Legacy Electronics Systems**
Faculty: Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585 and Nima Maghari, Domenic Forte, Swarup Bhunia, and Prabhat Mishra

*Project Description:* 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.

P56. **Securing Machine Learning Systems**
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093

*Project Description:* 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.
P57. **Securing Emerging Digital Financial Systems**  
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project description:** 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.

P58. **Protecting Data with Mandatory Retention Requirements**  
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project description:** 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.

P59. **Characterizing and Strengthening the Modern Health Ecosystem**  
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project description:** 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.

**P60. Enhancing Electronic Payment Security**  
Professor Patrick Traynor, traynor@cise.ufl.edu, 352-294-2093  
**Project description:** 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.

**P61. Electronic Payments are Essential to Our Modern Economy.**  
Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710  
**Project Summary:** 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.

**P62. An IoT Fingerprinting Framework Using Inherent Device Characteristics**  
Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710  
**Project Summary:** 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.

P63. **Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework**

Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710

**Project Summary:** 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).

P64. **Privacy-aware Wearable-Assisted Continuous Authentication Framework**

Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710

**Project Summary:** 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 is 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.
P65. **A Sustainable IoT Software Development Framework for Science and Engineering Researchers**  
Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710  
**Project Summary:** 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.

Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710  
**Project Summary:** 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 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.

P67. **Development of A Hands-on Security Class for Internet of Things**  
Professor Selcuk Uluagac, suluagac@fiu.edu, 1-305-348-3710  
**Project Summary:** 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.

P68. **Deep Learning for Identity Sciences**  
Professor Damon L. Woodard, dwoodard@ece.ufl.edu, 352-273-2130  
**Project description:** Deep learning has made a huge impact in various domains like Computer Vision, Natural Language Processing, and Speech processing. In this project, explore the relative merits and demerits of deep learning when applied to Identity Sciences domain. Identity science is the study of the use of physiological signals, cultural traits, behavioral interactions, digital artifacts, and emotion cues for establishing the identity of an individual or group. In a number of identity science applications, the identification of an individual within a set of candidates in the order of millions via a small set of samples is typical. Deep learning approaches can inherently learn discriminating features from raw data, and it would be useful to let the model learn features that could identify millions of people. However, deep learning approaches require large amounts of training data for every category owing to their complex architecture. In this project, we aim to identify options to leverage the feature learning capability of deep learning approaches for scenarios with few samples per person and a large number of categories. Some of the topics to be explored include:
- The use of Generative Models trained in an unsupervised manner to leverage feature learning from a small number of samples.
- Network growing approaches to improve the performance of deep learning on unseen data to improve generalization performance.

P69. **Automatic Author Attribution Via Stylometry**  
Professor Damon L. Woodard, dwoodard@ece.ufl.edu, 352-273-2130  
**Project description:** 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.
P70. **A Feasibility Study of Mobile Device Usage Data for Identification and Soft Biometric Classification**  
**Professor Damon L. Woodard, dwoodard@ece.ufl.edu, 352-273-2130**  
**Project description:** Mobile device usage consists of underlying behavioral patterns which may be exploited for identifying individuals. Because passwords, PINs, and patterns require frequent authentications and are easily stolen through observation or brute force, the ability to identify a mobile device user based on how the device is normally used provides a more secure and convenient locking mechanism. This project explores mobile device usage for identification and verification in regards to optimizing identification accuracy, mapping various usage patterns to certain demographics such as gender, and assessing the system vulnerability. This project is advantageous because future security disputes will occur largely in cyberspace where physical attributes are unavailable and/or unreliable. While many research efforts have demonstrated the effectiveness of mobile device data for verification, this project is more applicable to the needle-in-a-haystack problem. As the world become more connected online, it is expected that datasets which consist of cyber data from thousands to millions of individuals to emerge. Eventually, identification questions will also arise, such as “Which individual is most likely responsible for distributing this virus based on these web browsing logs?” or “Is this threatening email most likely written by a young male?” This work intends to examine possible behaviors in regards to mobile device usage which can assist in answering similar questions.

P71. **Hardware/Software Co-Verification for Security**  
**Professor Tuba Yavuz, tuba@ece.ufl.edu, 352-846-0202**  
**Project description:** 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.

P72. **A Formal Approach to Deception**  
**Professor Tuba Yavuz, tuba@ece.ufl.edu, 352-846-0202**  
**Project description:** 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.

P73. **Protection Against Optical Probing Attacks**  
**Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, and Navid Asadi, nasadi@ece.ufl.edu, 352-294-1075**  
**Project Description:** 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 instrument in the FICS facilities.

P74. HARDEN: Hardware-Assisted ML-based Anomaly Detection for Cyber Defense
Professors Mark Tehranipoor, tehranipoor@ufl.edu, 352-392-2585, and Yier Jin, yier.jin@ece.ufl.edu, 352-294-0401

Project Description: 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 module over time in response to new threats and attacks.
P75. IPTrust: A Comprehensive Framework for IP Integrity Validation
Professors Prabhat Mishra, prabhat@ufl.edu, Swarup Bhunia, swarup@ufl.edu and Yier Jin, yier.jin@ece.ufl.edu
Project Description: Reusable hardware Intellectual Property (IP) based System-on-Chip (SoC) design has emerged as a pervasive design practice in the industry to dramatically reduce design/verification cost while meeting aggressive time-to-market constraints. However, growing reliance on these pre-verified hardware IPs, often gathered from untrusted third-party vendors, severely affects the security and trustworthiness of SoC computing platforms. An important emerging concern with the hardware IPs acquired from external sources is that they may come with deliberate malicious implants to incorporate undesired functionality, undocumented test/debug interface working as hidden backdoor, or other integrity issues. In this project, we investigate a comprehensive scalable framework for IP trust verification through integration of trust analysis with a unified functional-structural-parametric trust validation scheme, and effective IP trust metrics.
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).
I. 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

II. 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 Oscilloscope; (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

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

III. 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://fics-institute.org/facilities/.
I: FERA-3 GMH Xe-Plasma FIB with Integrated Schottky

II: ORION NanoFab

III: Leica DVM6

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

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

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

**Introduction to Hardware Security and Trust.** (2012).
Tehranipoor, M. and Wang, C. *Springer*
Springer Publications

Tehranipoor, M and Salmani, H. *Springer*
Springer Publications

**Counterfeit Integrated Circuits.** (2015).
Tehranipoor, M., Guin, U. and Forte D.
Springer Publications
Hardware Protection through Obfuscation. (2017)

Hardware IP Security and Trust. (2017)
Mishra, P., Bhunia, S., and Tehranipoor, M. Springer Publications


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

The Hardware Trojans War. (2018)
Bhunia, S. and Tehranipoor, M. Springer Publications
FACULTY BIOS

Swarup Bhunia

Swarup Bhunia is the Education Director at FICS Research and is a Professor in the Department of Electrical and Computer Engineering (ECE) at the University of Florida. Dr. Bhunia received his B.E. (Hons.) from Jadavpur University, Kolkata, India, M.Tech. from the Indian Institute of Technology (IIT), Kharagpur, and Ph.D. from Purdue University, IN, USA. He co-founded the first-ever journal on hardware security, Journal of Hardware and Systems Security (HaSS). He currently leads research effort in Nanoscope, the nanocomputing research laboratory at the University of Florida.

Kevin Butler

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.

Domenic Forte

Domenic Forte is an Assistant Professor in the Department of Electrical and Computer Engineering. He received a PhD in Electrical and Computer Engineering from the University of Maryland in 2013. Dr. Forte is a recipient of the NSF CAREER Award (2017), Young Investigator Award (2015) by Army Research Office, and George Corcoran Memorial Outstanding Teaching Award (2008) by the Electrical and Computer Engineering Department at University of Maryland. He is co-author of one book, co-editor of two books, and has over 80 peer-reviewed publications in the area of hardware security.
Dr. 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.

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). Prior to joining UF, he was an assistant professor in the ECE Department at the University of Central Florida (UCF). He received his Ph.D 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. His research focuses on the areas of embedded systems design and security, trusted hardware intellectual property (IP) cores and hardware-software co-design for modern computing systems.

Dr. Xiaolin (Andy) Li is a Professor and University Term Professor in Department of Electrical and Computer Engineering (ECE) and Department of Computer & Information Science & Engineering (CISE, affiliated) at University of Florida (UF). His research interests include Cloud Computing, Big Data, Deep Learning, Intelligent Platforms, HPC, and Security & Privacy for Health, Precision Medicine, CPS/IoT, Science, Engineering, and Business. He is the founding Director of Large-scale Intelligent Systems Laboratory (Li Lab) and the founding Director of National Science Foundation Center for Big Learning (CBL) with UF, CMU, U. Oregon, and UMKC. He is a recipient of the National Science Foundation CAREER Award in 2010, the Internet2 Innovative Application Award in 2013, NSF I-Corps Top Team Award in 2015, Top Team (DeepBipolar) in the CAGI Challenge on detecting bipolar disorder in 2016, and best several paper awards.
An Assistant Professor at ECE department of University of Florida. His main area of research is analog/mixed-signal IC design and includes designing high performance analog-to-digital converters (ADC), digital-to-analog converter (DAC), phase-locked-loops (PLL), low power regulators (LDOs) and other mixed-signal circuits and systems.

Prabhat Mishra is a Professor in the Department of Computer and Information Science and Engineering at the University of Florida. His research has 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 the Deputy Editor-in-Chief of IET Computers & Digital Techniques, and as an Associate Editor of ACM TODAES, IEEE TVLSI and Springer JETTA. Prof. Mishra is an ACM Distinguished Scientist and a Senior Member of IEEE.

Daniela Oliveira is the Director of Diversity at FICS Research. She received her BS and MS degree in Computer Science from the Federal University of Minas Gerais in Brazil, 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. She received her PhD in Computer Science from the University of California at Davis, where she specialized in computer security and operating systems.
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.

Mark M. Tehranipoor is Co-director of FICS Research. Currently the Intel Charles E. Young Professor in Cybersecurity at the University of Florida. Prior to joining 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).

Patrick Traynor is Co-director of FICS Research. He 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 for Pennsylvania State University in 2008 and 2004, respectively, and his B.S. in Computer Science from the 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.
Dr. A. 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.

Dr. 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).

Dr. 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.