Alexander DeTrano

alexdetrano@gmail.com | 239-821-3995
Portland, OR

EDUCATION

NEW YORK UNIVERSITY
MS in Electrical Engineering
2015 | New York, NY

VILLANOVA UNIVERSITY
BS in Electrical Engineering
Minor in Mathematics
2010 | Villanova, PA

SKILLS

SOFTWARE
Verdi • DVE • DVT• JasperGold Formal Property Verification • JasperGold Security Path Verification

PROGRAMMING
Code Review:
SystemVerilog • Verilog • C • C++ x86 Assembly • ARM Assembly • Java Python

Code Writing:
Python • C • C++ • Bash • MATLAB LaTeX

EXPERIENCE

INTEL CORP | Security Researcher
June 2015 – Present | Hillsboro, OR

- Pre-silicon security assurance for Intel architectures across a variety of market segments (client chipset, wearables, IOT, automotive, artificial intelligence)
- Threat modeling, risk assessment, vulnerability analysis, design and implementation review for a number of Intel products
- Participate in hardware/firmware/software hackathons
- Recommend security vulnerability fixes and collaborate with cross-discipline teams in multiple geolocations to resolve security issues
- Developed a tool in Python to speed-up reviewing register files

INTEL CORP | Security Validation Engineering Intern
Jan 2015 – May 2015 | Hillsboro, OR

- Developed hardware security guidance for 3rd-Party IP (3PIP) providers. The guidance focused on actionable insights that a 3PIP provider with no security knowledge could use to reduce the most common pre-silicon bugs.
- The 3PIP HW security guidance was added as part of Intel's Secure Design Lifecycle.
- Developed a tool in Python which provided an easy way to validate IP assets

RESEARCH

ATTACKING A MASKED SOFTWARE IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD (AES) | NYU
2014 | New York, NY

- Recovered the secret encryption key from a masked implementation of AES-256 on an Atmel ATMega-163 smart-card using 15 power traces
- First attack targeted the loading of the masks from memory, and recovered the mask with 91% success
- Second attack identified collisions between two AES S-Boxes and recovered the difference between bytes of the key, reducing brute-force attack complexity from 2^{128} to 2^{8}
- Both attacks coded in MATLAB and were accepted to the DPA Contest V4.

PUBLICATIONS

[1] A. DeTrano, S. Guilley, X. Guo, N. Karimi, and R. Karri. Exploiting Small Leakages in Masks to Turn a Second-order Attack into a First-order Attack. In *Proceedings of the Fourth Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '15. ACM, 2015.