Hardware-Oriented Security and Trust (HOST)

Instructor:

Prof. Jim Plusquellic

Text:

- "The Hardware Trojan War: Attacks, Myths, and Defenses", Chapter 10, J. Plusquellic and F. Saqib, "Detecting Hardware Trojans using Delay Analysis", Springer, 2018, ISBN 978-3-319-68511-3, http://www.springer.com/us/book/9783319685106
- "Fundamentals of IP and SoC Security, Design, Verification, and Debug", Chapter 6, J. Plusquellic, "PUF-Based Authentication", Springer, ISBN 978-3-319-50057-7, http://www.springer.com/us/book/9783319500553
- "Physically Unclonable Functions: Constructions, Properties and Applications", Roel Maes, Springer, SBN 978-3-642-41394-0, ISBN 978-3-642-41395-7 (eBook)
- "Handbook of Applied Cryptography", A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, http://cacr.uwaterloo.ca/hac/

Web: http://www.ece.unm.edu/jimp/HOST

Course Goals

To investigate traditional and emerging hardware security and trust issues in all types of hardware systems at the chip- (ASICs, COTs and FPGAs), board- and system-level

Our trek through HOST topics will include

- Learning established cryptographic hardware algorithms and their implementation details
- Exploring security and trust approaches within RFID, smart-cards, autonomous vehicles, communications systems, etc. and the types of attacks that adversaries engage in to break them
- Investigating recent research activity in areas such as hardware Trojans, physical unclonable functions (PUFs), side-channel attacks, hardware obfuscation and board-level security.

With the objective of making you aware of hardware system vulnerabilities and techniques that can be used to address them early in the design cycle

In contrast to the 'patch' approach utilized in the past within commercial OS and software systems

Important Domain Knowledge

It is impossible to study hardware security and trust in isolation

HOST is cross-disciplinary and requires breath of knowledge in the following areas:

- Cryptography

  Mathematical methods designed to provide confidentiality and authenticity between communicating entities

- FPGA & VLSI Design Tools and Flows

  Computer-aided design (CAD) tools that enable designers to build chips and program FPGAs

- VLSI Testing

  Algorithms capable of generating high-coverage tests for ensuring that consumer chips are defect-free and meet performance constraints

- Probability and Statistics

  Mathematical techniques that enable characterization of data generated by complex hardware systems with un-modeled parameters

HOST Threats

The number of HOST threats continues to expand, some examples include:

- Side-channel attacks

  There are many types of attacks that have been developed to extract private information from chips, including simple power analysis (SPA), differential power analysis (DPA), correlation power analysis (CPA), etc.

- Trust in ASICs and FPGAs

  Adversaries can insert additional functionality (hardware Trojans or HT) in chips fabricated in untrusted foundries

  FPGA fabrics and bitstreams are vulnerable to malicious modifications

- IP piracy

  Adversaries can reverse-engineer ASICs and FPGA bitstreams and illegally use intellectual property developed by other companies

- Key generation and storage

  Adversaries can apply semi-invasive techniques to 'read out' secrets from non-volatile memories (NVM) -- most systems use keys as their 'root-of-security'

Recently Published HOST-Related Articles

"Comcast Security Flaw could help Burglars Break into Homes Undetected", Jon Brodkin, ARS Technica, Jan. 2016

"DHS, FBI Warn of Cyberattack Threat to Nation's Power Grid", April, 2016

"Hackers Remotely Kill a Jeep on the Highway - With Me in It", July, 2015

"How I Hacked An Electronic Voting Machine by By Roger Johnston", Nov, 2012

"The Hunt for the Kill Switch", IEEE Spectrum, May 2008

Presents anecdotal evidence of Hardware Trojans:

- Compromised microprocessors in Syrian radar system enabled Israeli jets to bomb suspected nuclear installation unhampered
- Inserted 'kill switch' in a microprocessor used by French defense contractor enables French to disable military equipment that falls into enemy hands

Countermeasures

Techniques are evolving to deal with these threats

- Trojan detection and localization methods in IP and ICs
- Physical unclonable functions (PUFs) for key generation and authentication
- FPGAs bitstream encryption/decryption schemes to prevent HT and IP theft
- Design obfuscation methods to increase the difficulty of reverse engineering
- Implementation techniques to prevent/deter differential power analysis
- Scan-chain encryption to prevent reverse engineering using side-channels
- Hardware security modules to prevent cable TV theft
- PCB-level methods to detect chip swapping