REALITY OF HARDWARE VULNERABILITY

Dr. Fouad Kiamilev
Furkan Cayci
Department of Electrical and Computer Engineering

Convergence of Software Assurance Methodologies and Trustworthy Semiconductor Design and Manufacture Workshop
January 15-16, 2013
Outline

- Hardware Examples
- Hardware Vulnerability
- Demonstration
- Conclusion
Hardware Example 2

- V2G-capable Electric Vehicle Charging Station
- Parts of design performed by foreign nationals
- Uses no custom integrated circuits
- Manufacturing of systems will be off-shore
- Market size: millions of units
- Product cost: $$$
- Product will be sold in the open market
- Parts of our design are becoming a standard – “open source”
What is V2G?

Grid Operator
ISO protocol

Aggregator

VMS
OEM Protocol

VSL
communication agent

VSL

VSL
communication agent

EVSE+
VEL

EVSE+
VEL

EVSE+
VEL

vehicle 1

evse 1

evse 2

vehicle 2

network
via wired, wireless, PLC, any means

mobile GPRS

Ethernet

J1772 Protocol
+ In-band digital

J1772 Protocol
+ In-band digital

OEM Protocol

CMOS VLSI Optimization Research Group
What is V2G?

- Bidirectional flow of information and power in and out of electric vehicles.

- Increased use in renewables and/or isolated power systems increases need for power storage.

- Electric vehicles can be leveraged by utilizing power electronics and batteries while car is parked.
This system is less secure because…

- Most of the parts of the system are external
Why is hardware vulnerability a threat?

- Electronics plays an important role in:
  - Storage and communication of confidential information
  - Management and control of important equipment
  - Critical national security applications and systems
- Globalization
What can it do?

- Malicious alteration of hardware, that could, under specific conditions, result in functional changes of the system
- Disable a system at some future time.
- Leak confidential information over a secret channel
What can be altered?

- Firmware
- HDL Source Code
- IC Layout
- Circuit Diagram
Scenario: Bank robbery!
No Witness?
No Worries! Watch the surveillance videos
Wait!!… What???
What actually happened…

- Tampered surveillance cameras

- A very specific trigger condition that is pre-defined in the firmware
  - A ‘unique’ signature

- Trojan activated to show a pre-stored image instead of the face of the thief
Action!
Platform

- **PowerShot SD1000 / Digital IXUS 70**
  - 7.1 Megapixel
  - DIGIC III Image Processor
  - VxWorks Operating System

- **Canon Hack Development Kit**
  - Temporary
  - Flexible
  - Free
Trojan Insertion

Diagram:

1. Lens → CCD → ADC → Image Processing → Malicious Module → Pattern
2. Pattern match? Yes → Decider Logic → Yes to Camera LCD Screen
3. Pattern match? No → Decider Logic → No to Camera Storage Card → Camera Output Port
Demo!
Conclusion

- We might need to look into the problem as a whole system
  - Any part is vulnerable, system is owned
- Cat and mouse
  - iOS jailbreak, MS Xbox, Crypto algorithms
- Cost-Vulnerability tradeoff
References

- Defcon 16: Hardware Trojan Demonstration - [http://www.cvorg.ece.udel.edu/defcon-16/](http://www.cvorg.ece.udel.edu/defcon-16/)

Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions, X. Wang, M. Tehranipoor, and J. Plusquellic, IEEE HOST 2008 Workshop, Anaheim, California, USA