Introduction to Hardware Security

Engr 399/599: Hardware Security

Grant Skipper
Indiana University

Adapted from: Mark Tehranipoor of University of Florida

Course Website

engr599.github.io

Write that down!

Why Hardware Security?

- ***Cybersecurity experts have traditionally assumed that the hardware underlying information systems is secure and trusted.***

- ***Such assumptions are not true.***

The goals of this class are to:

- Learn the state-of-the-art security primitives and methods
- Integration of security as a design metric
- Protection of the design intellectual property against piracy and tampering
- Understanding of attacks and countermeasures
- Understanding of vulnerabilities in design and fabrication processes

Course Topics

- Hardware Security and Trust
- Hardware Cryptography
- Physically-Unclonable Functions (PUFs)
- True Random Number Generation (TRNG)
- Hardware Metering and Watermarking
- Hardware Physical and Fault-Injection Attacks
- Hardware Trojans
- Counterfeit Detection
- Side Channel Analysis
- FPGA Security
- PCB Security

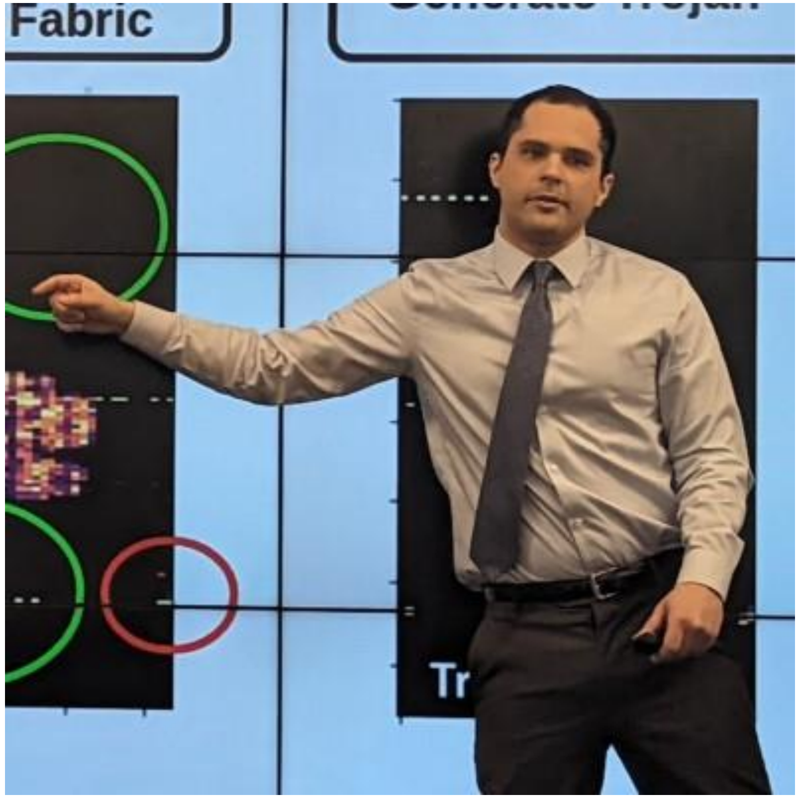
About Me - Professor

Grant Skipper, Microelectronic Security Engineer

Office Hours: Monday and Wednesday, TBD on time

Main research work is on security for FPGA-based systems, hardware Trojans, and embedded devices

Ph.D. in Intelligent Systems Engineering from IU - 2022



About Chris - TA

Chris Sozio, Ph.D. student in Intelligent Systems Engineering

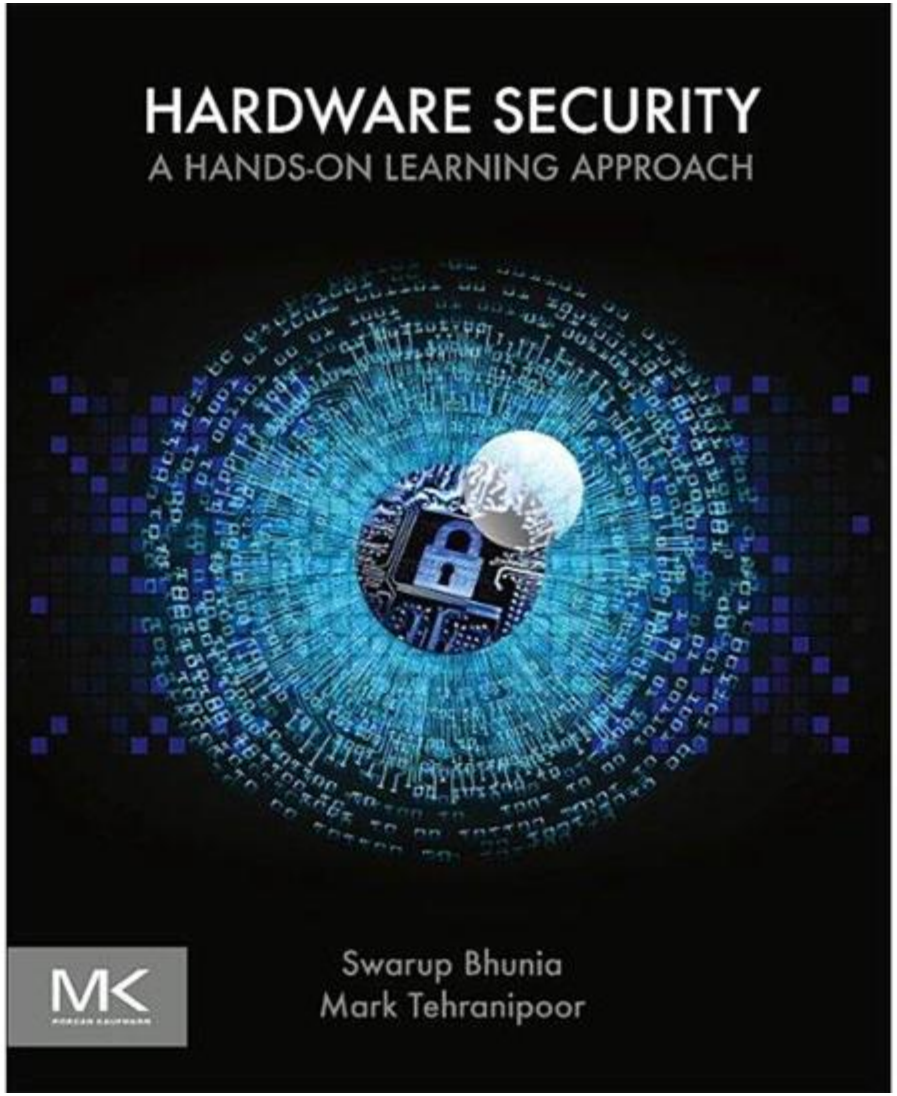
Office Hours: TBD

Main research work is on security for FPGA-based systems, and hardware Trojans

B.S. in Computer Science from IU - 2019

About You?

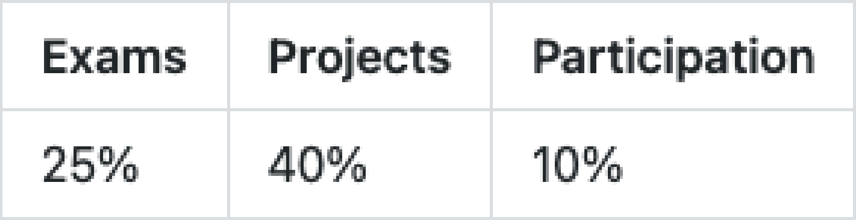
- Name
- Year / Department
- Why did you take this class?
- What are you hoping to learn?
- What’s your background? Cybersecurity? Hardware?



- Available online through IU’s Library (See syllabus)

Grading

- The syllabus currently says this:



Exams	Projects	Participation
25%	40%	10%

- This might change. We’re still working out the projects.

A note on the slides

- These slides are adapted from an equivalent course at the University of Florida

- They are dense

- Please stop me and ask questions

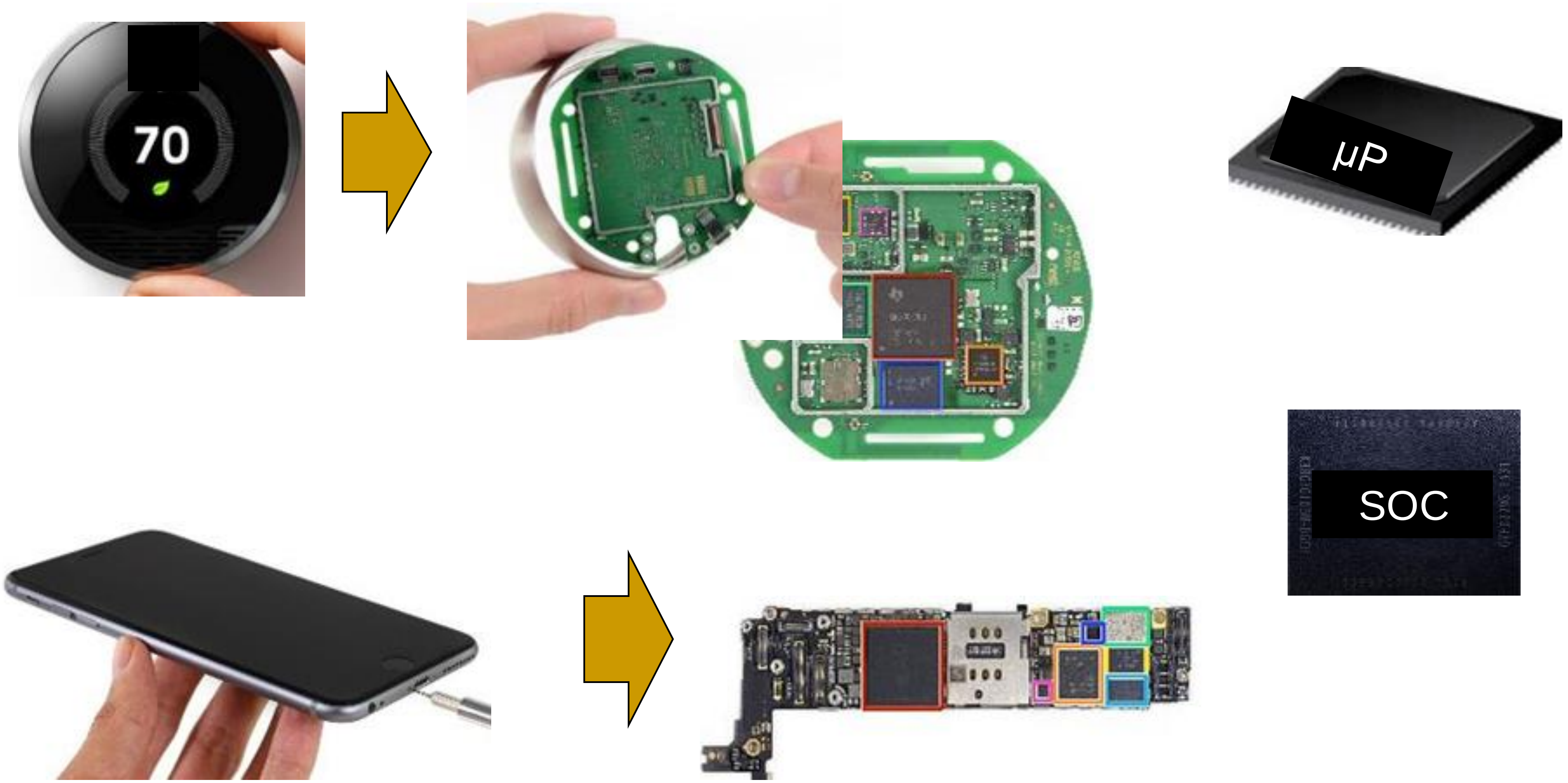
More to Read …

- **Reading**
  - Papers from the contemporary literature
- Further possible reading
  - Mihir Bellare and Phil Rogaway, **Introduction to Modern Cryptography**
  - Ross J. Anderson. **Security Engineering: A guide to building dependable distributed systems**. John Wiley and Sons, 2001
  - Matt Bishop, **Computer Security: Art and Science**, Addison-Wesley, 2003
  - William Stallings. **Cryptography and Network Security**, Fourth edition, 2007
  - M. Tehranipoor and F. Koushanfar, "**A Survey of Hardware Trojan Taxonomy and Detection**," IEEE Design and Test of Computers, 2010.
  - M. Tehranipoor, H. Salmani, and X. Zhang, **Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection**, Springer July 2013.
  - U. Guin, D. DiMase, and M. Tehranipoor, “**Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead**,” Journal of Electronic Testing: Theory and Applications (**JETTA**), Feb. 2014.

More to Watch!

- **Videos**
  - What's inside a microchip? http://www.youtube.com/watch?v=GdqbLmdKgw4
  - Zoom Into a Microchip http://www.youtube.com/watch?v=Fxv3JoS1uY8
  - Public Key Cryptography: RSA Encryption: http://www.youtube.com/watch?v=wXB-V_Keiu8
  - Counterfeit Electronics Could Be Dangerous, Funding Nefarious People http://www.youtube.com/watch?v=dbZiUe6guxc
  - How Computers and Electronics Are Recycled http://www.youtube.com/watch?v=Iw4g6H7alvo
  - Counterfeit Electronic Components Process http://www.youtube.com/watch?v=5vN_7NJ4qYA
  - Counterfeit Inspection http://www.youtube.com/watch?v=MbQUvu2LN6o
  - Gold from waste circuit electronics http://www.youtube.com/watch?v=ZkhOuNvkuu8
  - Tarnovsky Deconstruct Processor https://www.youtube.com/watch?v=w7PT0nrK2BE

What is Hardware?



- Electronic System
- System Hardware – acts as the ***“root-of-trust”***: PCB → IC (SoC | μP)

What is a “Root-of-Trust”?

Example Attack

Roy Zoppoth stands over a Xerox 914 copy machine, the world's first, which was used in soviet embassies all over the world. The machine was so complex that the CIA used a tiny camera designed by Zoppoth to capture documents copied on the machine by the soviets and retrieved them using a "Xerox repairman" right under the eyes of soviet security.

Photo from edit international courtesy of Roy Zoppoth

Motivation – HW Security

- **HW security is becoming increasingly important**
  - Hardware security sneaks into PCs, Robert Lemos, CNET News.com, 3/16/05
  - Microsoft reveals hardware security plans, concerns remain, Robert Lemos, SecurityFocus 04/26/05
  - Princeton Professor Finds No Hardware Security In E-Voting Machine, Antone Gonsalves, InformationWeek 02/16/07
  - Secure Chips for Gadgets Set to Soar, John P. Mello Jr. TechNewsWorld, 05/16/07
  - Army requires security hardware for all PCs, Cheryl Gerber, FCW.com, 7/31/2006
  - Visit Facebook group on Hardware Security

Example Attack

Pentagon’s ‘Kill Switch': Urban Myth?

The Pentagon is worried that "backdoors" in computer processors might leave the American military vulnerable to an instant electronic shut-down. Those fears only grew, after an Israeli strike on an alleged nuclear facility in Syria. Many speculated that Syrian air defenses had been sabotaged by chips with a built-in ‘kill switch" — commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar."

This all had a very familiar ring to it. Those with long memories may also recall exactly the same scenario before: air defenses knocked out by the secret activation of code smuggled though in commercial hardware.

This was back in 1991 and the first Iraq War, when the knockout blow was administered by a virus carried by a printer : One printer, one virus, one disabled Iraqi air defense.

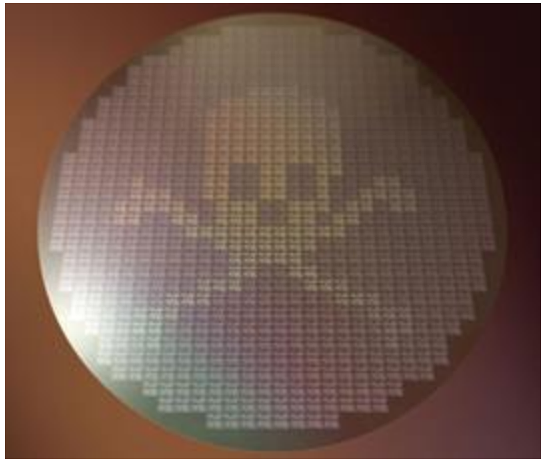
Example Attack

DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools

- Top homeland securities have admitted instances where along with software, hardware components that are being imported from foreign parties and used in different US systems are being compromised and altered to enable easier cyber-attacks.

The Hunt for Kill Switch, IEEE Spectrum 2008

- Increasing threat to hardware due to globalization
- Extremely difficult to detect kill switches (utilized by enemies to damage/destroy opponent artillery during critical missions) as well as intentional backdoors (to enable remote control of chips without user knowledge), which may have huge consequences
- Example: Syrian’s Radar during Israeli attack, French Government using kill switches intentionally as a form of active defense to damage the chips if they fall in hostile hands, and more…



Example Attack

Fake Cisco routers risk "IT subversion”

- An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors.
- $76 million **fake Cisco routers**

Energy Theft Going From Bad to Worse

- Tampering with “smart” meters
  - Oil, electricity, gas, …
- $1B loss in CT because of electricity theft

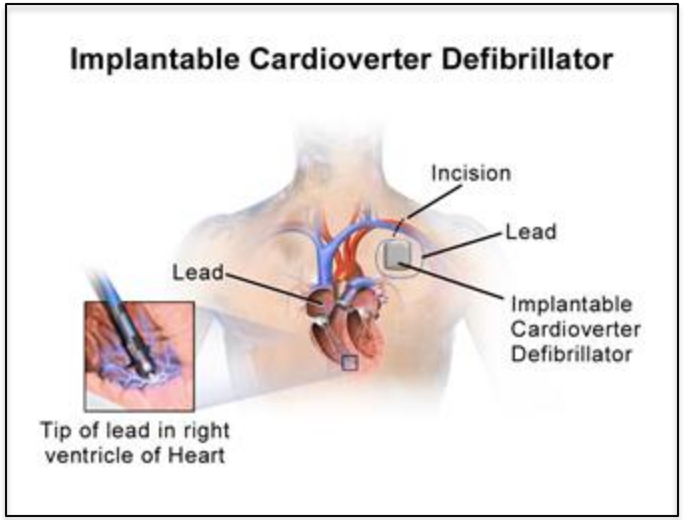
Example Attack

The deadly world of fake medicine – CNN.com

- A **counterfeit medication** or a counterfeit drug is a medication or pharmaceutical product which is produced and sold with the intent to deceptively represent its origin, authenticity or effectiveness.

Medical Device Security

- Incorporating security is sometimes considered expensive
- Implantable devices: e.g., Heart rate monitor
  - Incorporating Security could potentially reduce the life-time of the device by 30%
  - Attacking these device could result in loss of lives


Implantable Cardioverter Defibrillator
Incision
Lead
Lead
Implantable Cardioverter Defibrillator
Tip of lead in right ventricle of Heart

Example Attack

Physical Attacks on Chip IDs

- Extracting secret keys

Side-Channel Attacks

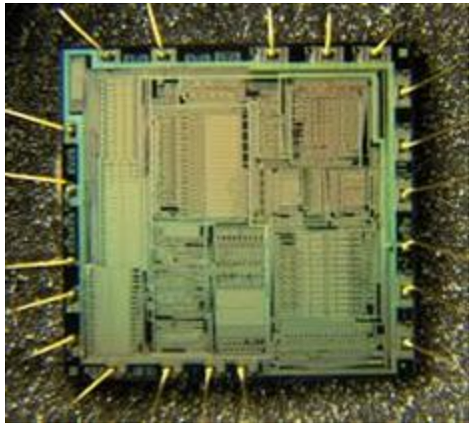
- Power Analysis, Timing Analysis, EM Analysis

Tampering with Electronic Devices

- Captured Drone by Iran

Counterfeit Integrated Circuits

- Multi-billion dollar business



IEEE
SPECTRUM
FAKE
Scavenged chips passed off as new are cropping up in U.S. military equipment.
Are they in passenger jets and cars, too? P. 40
IEEE