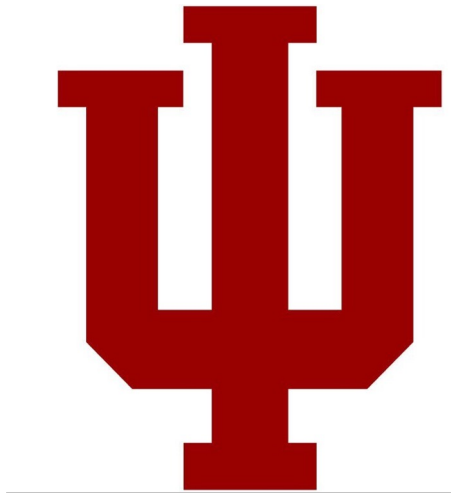
Hardware Security Papers

Engr 399/599: Hardware Security

Andrew Lukefahr
Indiana University



Adapted from: Mark Tehranipoor of University of Florida

Exam

- I have not yet looked at it.
- Starting grading on Tuesday.

Paper Presentations

Each group gets to present 2 papers

- We'll pick them in a little while.
- I have a suggested list, but feel free to suggest your own.

Non-presenting individuals:

- Read the paper before class
- Submit short write up to canvas
- Come to discuss

Canvas Writeup (1 sentence/ question)

- What's the problem?
- Why is it important?
- What did this paper do about it?

Presenting Group

- 20 minute presentation
- Shared between group

Suggested Presentation Slides

- Title – 1 slide
- Big Picture – 1 slide
- Overview – 1 slide
- Intro – 3 slides
- Overview – 1 slide
- Meat – 10 slides
- Overview – 1 slide
- Results/Graphs – 3 slides
- Overview – 1 slide
- Conclusions – 2 slides

Title – 1 slide

- Paper title
- Paper authors

- Presentation authors

Big Picture – 1 slide

- What's the problem?
- Why does it matter?
- What are the author's going to do about it?

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Introduction – 3 slides

- How did we get here?
- Why is this problem important to solve?
- What background do I need to know?

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Meat – 10 slides

- How does the system work?
- Figures / Diagrams are helpful here.
- Sub-sections are also useful.

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Results / Graphs - 3 slides

- Does it work?

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Conclusion – 1 slide

- What did I learn?
- What do you (presenter) think of paper?
- What do you (presenter) think we should do next?

Starbleed (2019) - https://www.usenix.org/conference/usenixsecurity20/presentation/ender

MORPHEUS (2019) - https://web.eecs.umich.edu/~barisk/public/morpheus.pdf

Side-Channel Analysis of the Xilinx Zynq UltraScale+ Encryption Engine (2021) - https://pdfs.semanticscholar.org/100d/983ed1192e1274dd71558eef30b352fa0dc5.pdf

Insights into the Mind of a Trojan Designer (2019) - https://arxiv.org/pdf/1910.01517.pdf

Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs

PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon

ThrAngry Cat – Cisco routers: https://redballoonsecurity.com/files/CycIhULVL5FS6VNM/100_seconds_of_solitude.pdf

- VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface (2021) - https://www.usenix.org/conference/usenixsecurity21/presentation/chen-zitai
- Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives (2019) - https://ieeexplore.ieee.org/abstract/document/8835339
- Golden Gates: A New Hybrid Approach for Rapid Hardware Trojan Detection using Testing and Imaging (2019) - https://ieeexplore.ieee.org/document/8741031
- Toward a Hardware Man-in-the-Middle Attack on PCIe Bus for Smart Data Replay (2020) - https://ieeexplore.ieee.org/document/8875023
- On the Usability of Authenticity Checks for Hardware Security Tokens (2021) - https://www.usenix.org/conference/usenixsecurity21/presentation/pfeffer
- A2: Analog Malicious Hardware (2016) - https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf
- Spectre Attacks: Exploiting Speculative Execution - https://ieeexplore.ieee.org/document/8835233

04/02	Tuesday	Group 5n(startbleed)
04/04	Thursday	Group 4(VoltPiligar) + Group 3(PCIe)
04/09	Tuesday	Group 2(US+) + Group 1(HW Tokens)
04/11	Thursday	OFFICE HOURS
04/16	Tuesday	Group 4 (SSDs) + Group 5 (ThrAngryCat)
04/18	Thursday	Group 3 (Golden) + Group 1 (PUFs)
04/23	Tuesday	Group 2 (Spectre)
04/25	Thursday	NO CLASS

- Group 1 — Tuesday – tokens
- Group 2 — Tuesday – Zynq
- Group 3 — Thursday – PCIe
- Group 4 — Thursday – ~~[illegible]~~ Volti Pilisan
- Group 5 — Tuesday (+2%) – Stabbed

Spectre

17 Mistakes Microsoft Made in the Xbox Security System

- https://events.ccc.de/congress/2005/fahrplan/attachments/674-slides_xbox.pdf

Things to improve:

- more involved labs
- redundant topics / slides
- protocols / hw chips

more algos

Intro to math of cyber security

C231