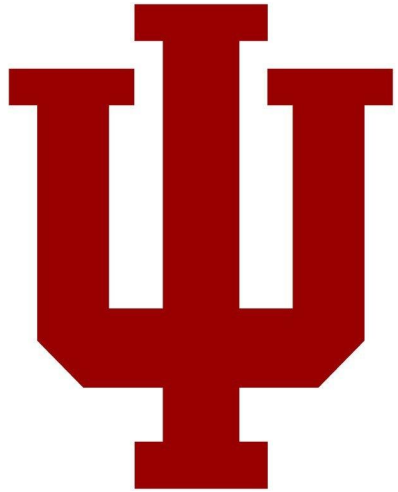
Hardware Security Papers

Engr 399/599: Hardware Security

Dr. Grant Skipper
Indiana University



Adapted from: Mark Tehranipoor of University of Florida

Paper Presentations

This is your Final Exam!!

Papers

- For final stretch of the semester, we'll be reading papers

- Each group (one-two) will present one paper.

Each Group gets to present ONE papers

- We'll pick them in a little while.
- From suggested list, exceptions possible

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

- 45 minute presentation (!!!)
- Shared between the 1-2 of you!

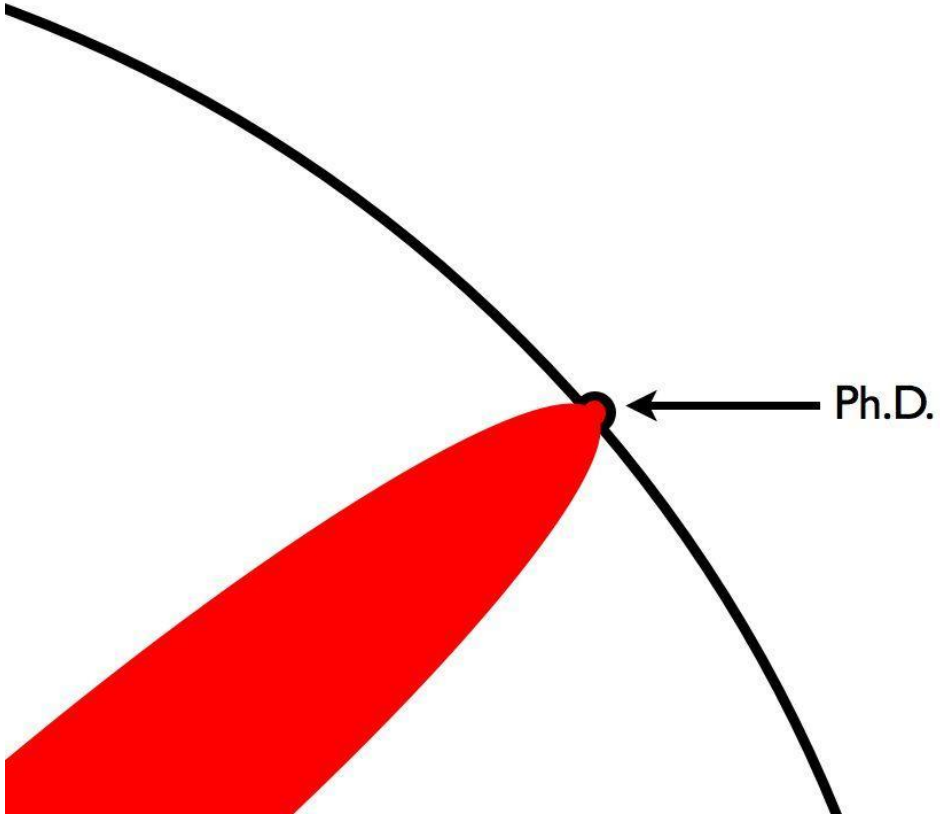
Assignments for Class (Non-Presenters)

- Listen to presentation.
- Answer 3 questions (per presentation, on Canvas).
  - What's the problem?
  - Why is it important?
  - What did this paper do about it?

Paper Reviews

- What is the problem?
- Why is it important?
- What are key assumptions that this paper makes?
- What are the main strengths of this paper?
- What are the main weaknesses of this paper?
- Which figure or experiment was most compelling in support of the hypothesis, and why?

illustrated guide to paper reading



- Taken from: http://matt.might.net/articles/phd-school-in-pictures/

Reading Papers is **HARD**

- Papers are about advancing current state-of-the-art
- Authors have been working on this for 30+ years
- You are just learning them
  - Big knowledge gap to fill quickly ☹️

Reading Papers takes **TIME**

- ~2 hours / paper
- Longer at first, faster over time
- You won’t understanding everything right away
  - Don’t try!

Reading Papers is a **PROCESS**

- Find “the problem”
- Find “why it matters”
- Find “the solution”
- Understand details only if needed

Papers have a **FORM**

- Papers have a form or template

- Abstract
- Introduction
- Background (Related Works)
- Body
- Results
- Conclusion

Abstract

- What is the **problem**?
- Why is it **important**?
- How did you **help**?

- 2 paragraphs

Introduction (Abstract++)

- What is the **problem**?
  - Super-fast background on problem
  - Why today's solutions aren't good enough?
  - What can we exploit to make it better?
- Why is it **important**?
  - Why should I care if you solved X
- How did you **help**?
  - What is different about your approach?
  - What are your main contributions to the field?
- Results

- 1-2 pages

Background (or Related Works)

- Background: what the authors think others need to know about the particular problem they are working on
  - Important section when reading papers in unfamiliar area
  - Usually ignored by domain experts

- Related Works: a bunch of people the authors needed to cite so they wouldn't be mad
  - Sometimes helpful if reading in unfamiliar area

- 1-2 pages

Body

- Nuts and bolts of your solution
- Implementation details

- Convince other domain experts you are right
- Confuse non-domain experts until they stop caring

- 3-6 pages

Results

- Illustrate your solution actually helps
- Convince domain experts you improved things
- Lets non-domain experts recover by looking at pretty graphs
- READ THE CAPTIONS!
- 2-4 pages

Conclusion

- Restated abstract with past-tense
- What we should do with this new knowledge

Other Sections

- You might also find:

- Experimental Setup / Methodology
  - Details about the experimental setup
- Acknowledgements
  - Who actually paid for the work
- Future Work
  - We know this work has problems. We might/might not work more on this in the future

Reading Papers is a **PROCESS**

- Multi-pass approach
  - 1) Scout Pass
  - 2) Trusting Pass
  - 3) Scrutinize Pass

1st Pass

- Get the general idea of the paper quickly
- 5-10 minutes

- Read:
  - Title
  - Abstract
  - Introduction
  - Section / Sub-Section headings (not paragraphs)
  - Graph captions
  - Conclusion

2nd Pass

- ~1-2 hours

- Read everything
- Assume the authors are correct

- Understand how their contribution works

- Sometimes you have “ah-ha” moments here

3rd Pass

- 2+ hours

- Can I mentally re-create their work?
- What are the authors hoping you don't notice?

- Mostly for reviewing papers
- Don't need to do this for this class.

Well written papers should answer these questions:

- What is the problem?
- Why is it important?
- What are key assumptions that this paper makes?
- What are the main strengths of this paper?
- What are the main weaknesses of this paper?
- Which figure or experiment was most compelling in support of the hypothesis, and why?

Some papers are better than others

- Don’t be surprised to find less helpful papers

- There are usually clues
  - What conference published the paper?
  - What universities/companies are the authors from?
  - Polish/clarity of the paper’s figures

For Today

- **17 Mistakes Microsoft Made in the Xbox Security System**

- Read it
- Come prepared to talk about it
- See if you can make me say “I don’t know”

Suggested Presentation Slides

- Title – 1 slide
- Big Picture – 1 slide
- Overview – 1 slide
- Intro – 7 slides
- Overview – 1 slide
- Meat – 20 slides
- Overview – 1 slide
- Results/Graphs – 5 slides
- Overview – 1 slide
- Conclusions – 3 slides

Title – 1 slide

- Paper title
- Paper authors
  - Who they are, where are they from, any interesting background?
  - Be a detective!
- Presentation authors

Big Picture – 1 slide

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

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Introduction – 7 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 – 20 slides

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

Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

Results / Graphs - 5 slides

- Does it work?
- Summarizing thoughts?

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?
- Does any derivative work exist?
  - How does the conversation continue?

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

FLATS: Filling Logic and Testing Spatially for FPGA Authentication and Tamper Detection (2019) - https://ieeexplore.ieee.org/abstract/document/8741025

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

Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems (2023)
ReCon: From the Bitstream to Piracy Detection (2020)

FANCI: identification of stealthy malicious logic using boolean functional analysis (2013)

Library-Attack: Reverse Engineering Approach for Evaluating Hardware IP Protection (2025)

Reflections on Trusting TrustHUB (2023)

- Monday
- Wednesday

- John:
- Spencer:
- Nate:
- Franklin:
- Aidan:
- Ben: