Security mini-panel

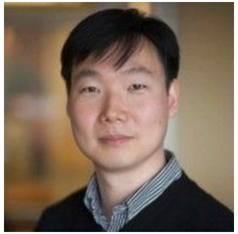
e-ISCA

1:45p EDT June 1, 2020

Panelists

Chris Fletcher
Assistant Professor, UIUC

Caroline Trippel
Assistant Professor, Stanford



Ed Suh
Professor, Cornell

Frank Mckeen
Security/Computer Architect, Intel

Panel format and purpose

Goal: what's next, and what is our community's role, in processor security?

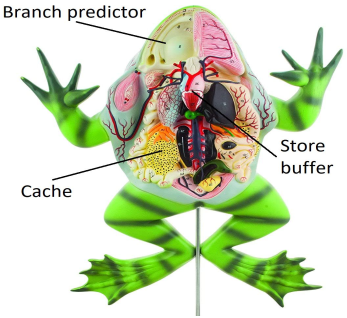
Format:
1.) Opening statements.
2.) Open to discussion. **Audience please submit questions via zoom/whova!**

Some examples:
What are computer architects' roles in finding new attacks?
Is the way we design computers fundamentally ill-equipped to deal with security?
What is the role of formal methods in designing secure hardware?
What is the role of computer architecture (and comp. architects) in security?

Opening statement - Chris

A lot of my time: “verifiable defenses”: security property → abstractions/interfaces → implementations → (hopefully someday) automatically verified

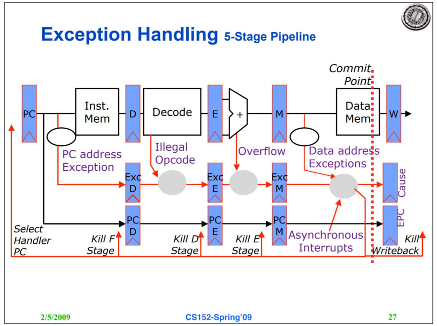
Today: Computer Architects should be the ones to find the next major uarch attack



Most attack research

https://cyber.wtf/author/andersfogh1974/

“Behind the scenes of a bug collision”



Exception Handling 5-Stage Pipeline

2/5/2009 CS152-Spring’09 27

My ugrad comp arch class

Computer Architecture is about exploiting the common case.

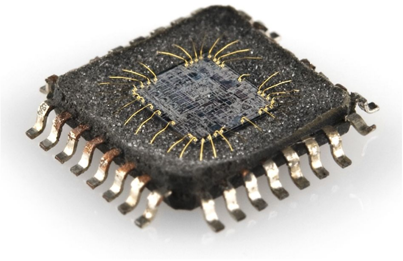
Processor Security is about what cool things happen (good or bad) when you induce the worst case.

Opening statement - Caroline

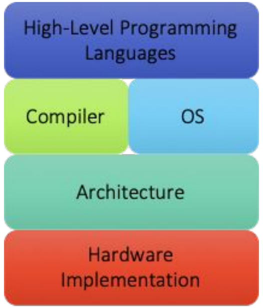
Themes of my current work: security as a first-order computer architecture design constraint · formal methods for computer architecture · formal security verification · interface specifications for security · application specific security

Today: The complexity of both modern microprocessor designs and hardware security vulnerabilities requires computer architects to devise mechanisms for enabling formal, automated security verification.

Design for security verification



Interface specs. for security



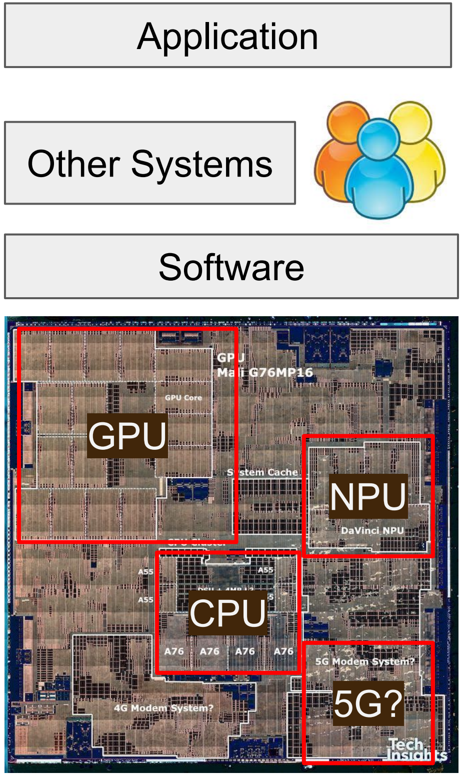
Application-specific security

Application-Driven, Full-System, Security Assurance

Today's research: Largely driven by **known attacks** on **general-purpose CPUs** with **empirical** security evaluation

Challenge/Opportunity: abstractions, interfaces, and mechanisms, and tools for **full-system assurance for application-level security properties**

- Abstractions and interfaces for HW-SW, HW-HW: hide implementation, composable security
- Architecture and tools for formal security assurance
- Assurance for users and other systems
- Application-driven: new security properties, specialized protection for lower overhead and complexity



Application

Other Systems

Software