Supply Chain Security Workshop

April 28 & 29, 2021

MEPTEC
THE NEXT GENERATION

www.meptec.org

Hardware and Supply Chain Security in the Era of Advanced Heterogenous Integration

MEPTEC Supply Chain Security Workshop, April 2021.

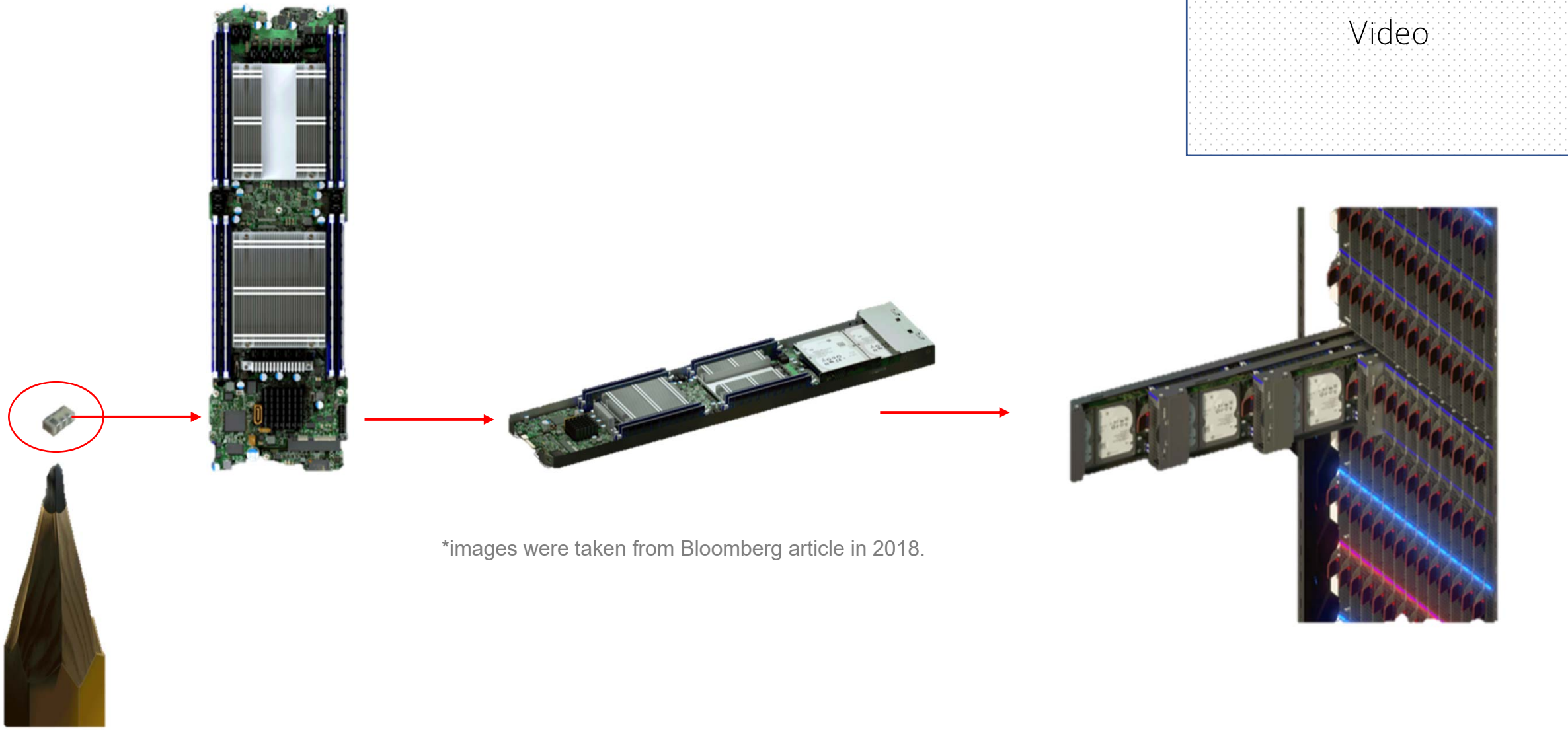
Nader Sehatbakhsh
Department of Electrical and Computer Engineering
University of California, Los Angeles

Video

- Let's start with a story…

UCLA Samueli School of Engineering

Video



*images were taken from Bloomberg article in 2018.

UCLA Samueli School of Engineering

Who were impacted?

Video

- AWS Servers
- Apple devices
- National Labs
- …

UCLA Samueli School of Engineering

Other Incidents?

Video

- *Quite a few …*

- Some where not confirmed, but technically possible, *so who knows?*

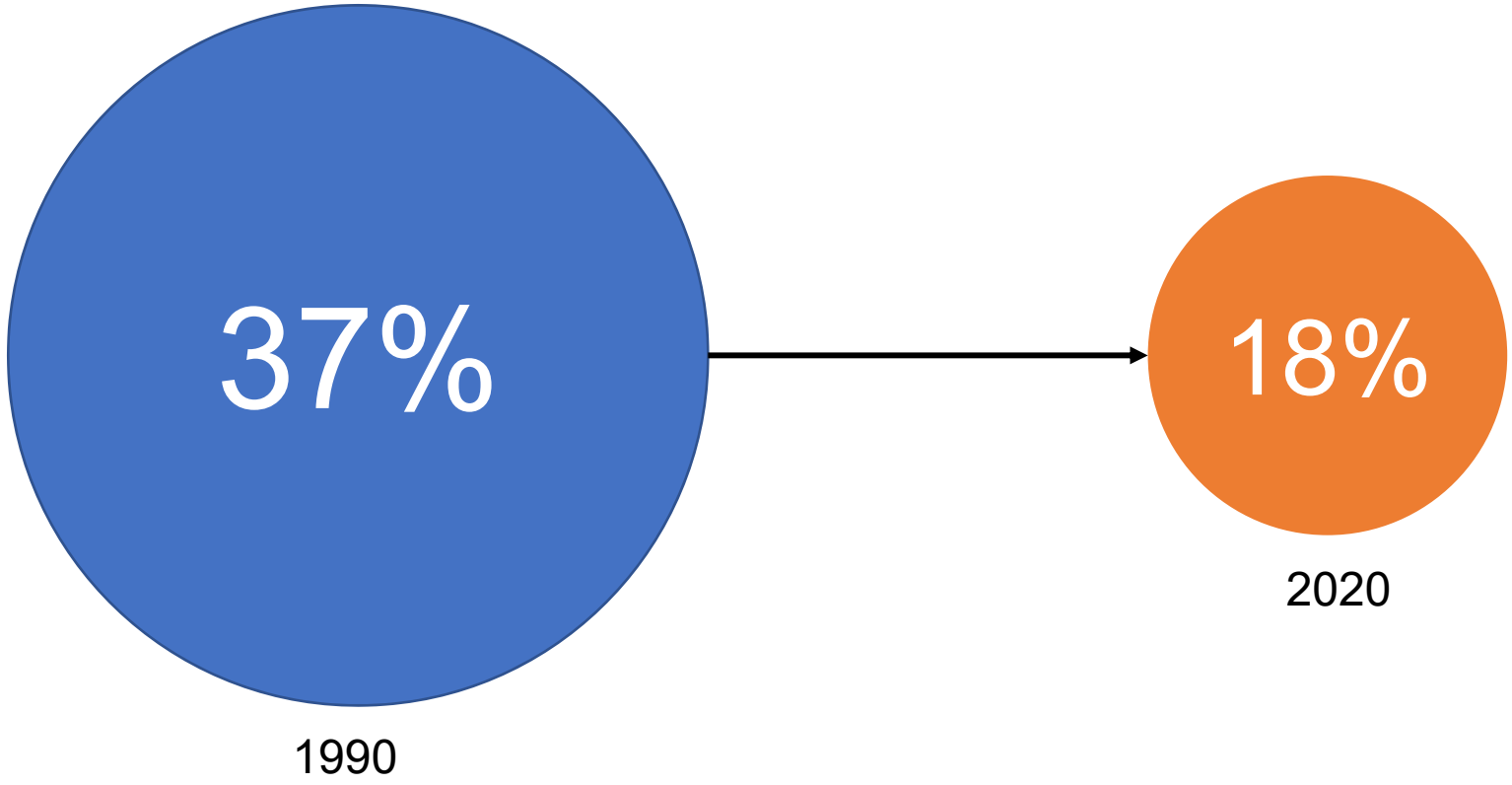
UCLA Samueli School of Engineering

Video

UCLA Samueli School of Engineering

US Global Chip Production Market Share

Video

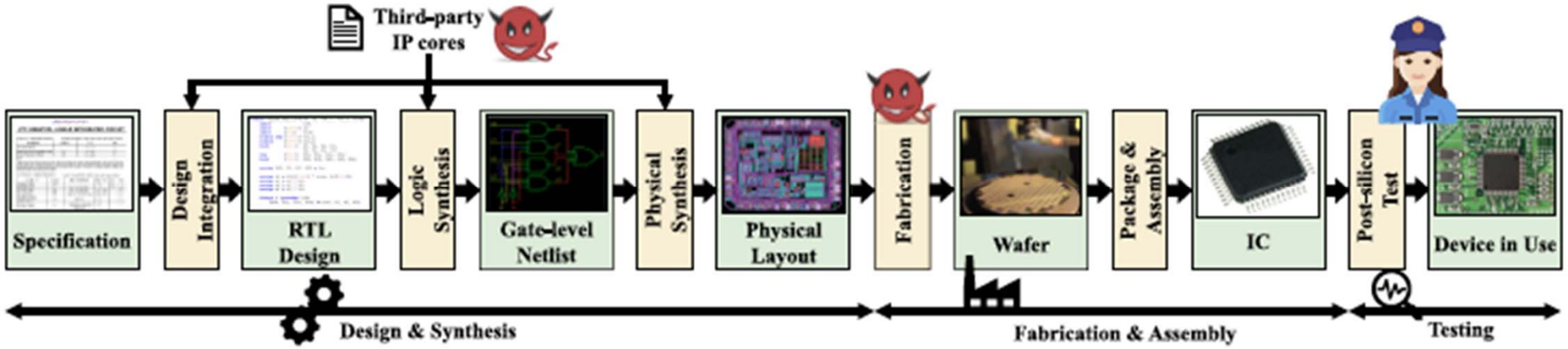


UCLA Samueli School of Engineering

So, What could *possibly* go wrong?

Video

- Hardware *Trojans*!



*images were taken from Faezi et al., “Brain-Inspired Golden Chip Free Hardware Trojan Detection,” TIFS’21.

Is get any better?

- ***NO!***

Video

UCLA Samueli School of Engineering

Is get any better?

Video

- ***NO!***

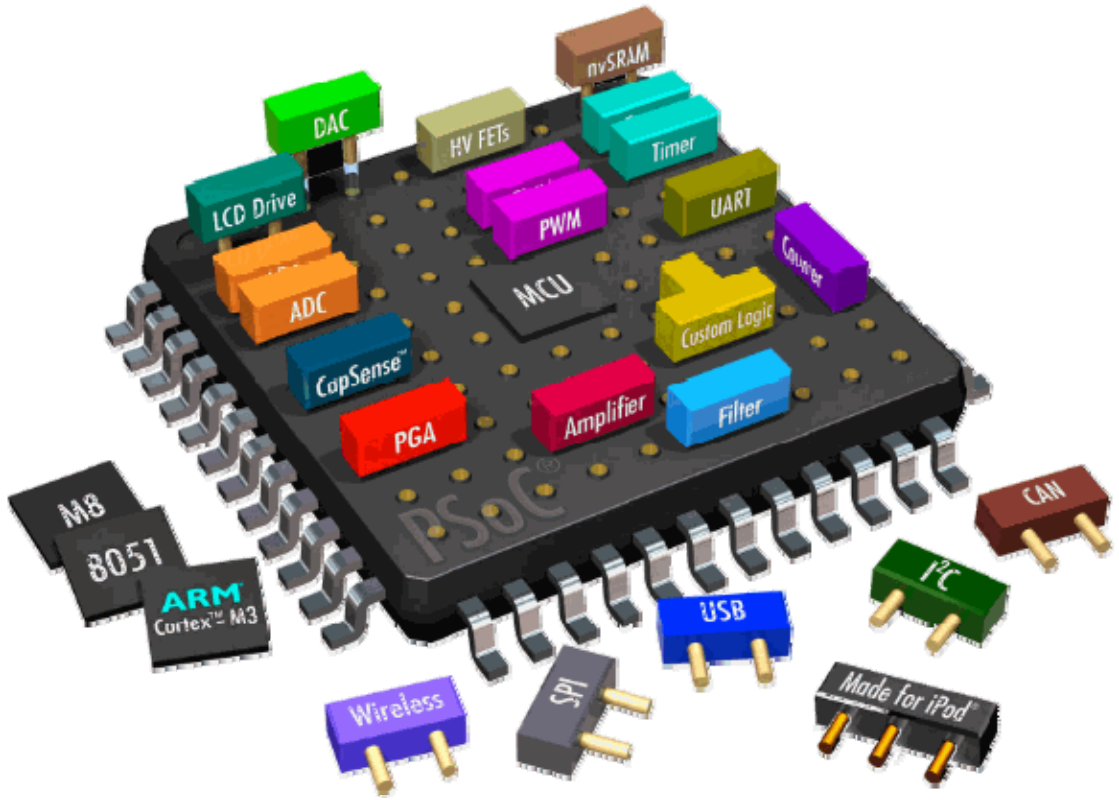
-- *Why?*

Even more heterogenous technologies.

- *Complex SoCs*
- *Motherboards*
- ***Dielets/Chiplets***

UCLA Samueli School of Engineering

Future Systems



*images were taken from https://microcontrollerslab.com/system-on-chip-soc-introduction/.

Video

- *Integrated* either on the
  - (i) same chip
  - (ii) same silicon die
  - (iii) on a PCB

Formulating the Problem

- Two *issues*:

  1- Individual chips *cannot* be trusted *(known unknown)*.

Video

Formulating the Problem

- Two *issues*:

  1- Individual chips *cannot* be trusted *(known unknown)*.

  2- Due to complexity of the system, the adversary *can add extra functionalities/chips* to the system. (*unknown unknown*).

Video

What can we do?

Video

UCLA Samueli School of Engineering

What can we do?

Video

- Define the ‘trust model’ – *who can/cannot we trust?*

UCLA Samueli School of Engineering

What can we do?

Video

- Define the ‘trust model’
  - Can we trust the foundry?
  - Can we trust the designer?

UCLA Samueli School of Engineering

What can we do?

Video

- Define the ‘trust model’
  - Can we trust the foundry?
  - Can we trust the designer?

- What do we have?
  - ‘Golden’ Model?
  - Design files?
  - Many samples of the same chip?

UCLA Samueli School of Engineering

State-of-the-Art Trojan Detection

Video

- Reverse-Engineering / Physical Inspection
  - Imaging
  - Functional/netlist extraction

State-of-the-Art Trojan Detection

Video

- Reverse-Engineering / Physical Inspection
  - Imaging
  - Functional/netlist extraction

-- Very effective for extracting Trojans

-- Destructive/Semi-Destructive

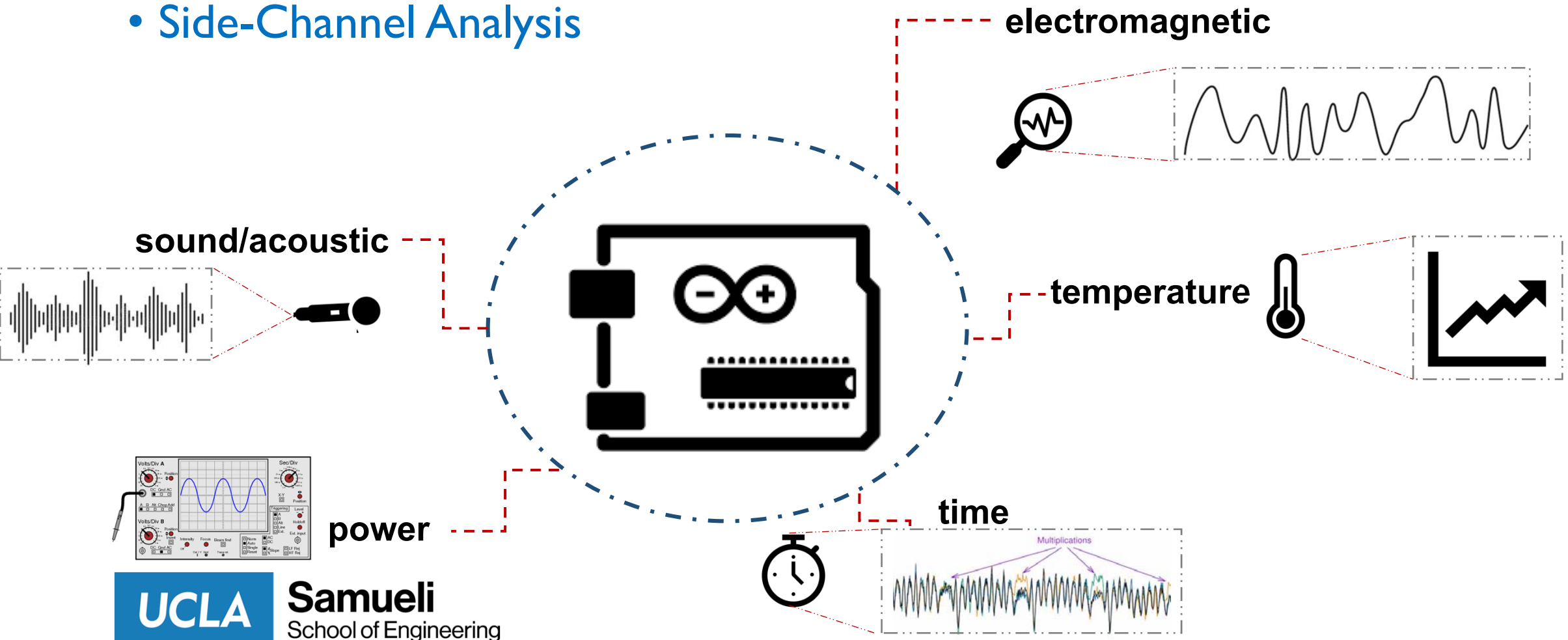
-- May need sophisticated equipment

UCLA Samueli School of Engineering

State-of-the-Art Trojan Detection

Video

- Side-Channel Analysis



UCLA Samueli School of Engineering

State-of-the-Art Trojan Detection

Video

- Side-Channel Analysis

  -- *Non-Destructive / low-cost*

  -- *Cannot detect subtle changes*

UCLA Samueli School of Engineering

Current Challenges

Video

- IF a golden-chip is *available*:
  - Testing results can be compared to a *reference*.

-- What if such a model is not available?

UCLA Samueli School of Engineering

Current Challenges

Video

- We can find known-unknowns (e.g., a modification in a given chip), but *how about unknown-unknowns?*

UCLA Samueli School of Engineering

Current Challenges

Video

- We can find known-unknowns (e.g., a modification in a given chip), but *how about unknown-unknowns?*

-- Dielet-Level / Motherboard-Level Security and Detection

UCLA Samueli School of Engineering

Research@UCLA

Video

- Finding new methods to tackle these challenges.

– *Two main research questions:*
  - *How to utilize side-channel in a golden-chip-free setting?*
  - *New hardware/software methods for dielet security?*

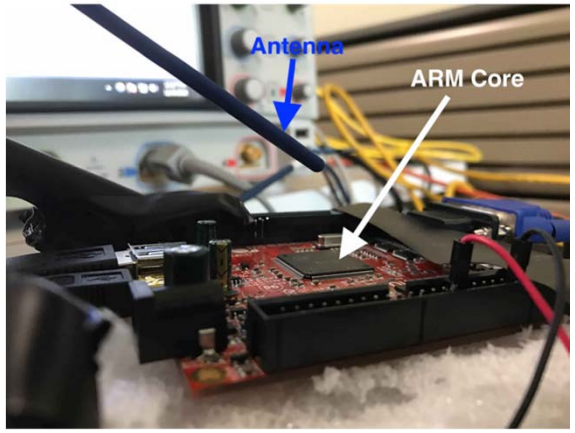
CHIPS
CENTER FOR HETEROGENEOUS INTEGRATION AND PERFORMANCE SCALING

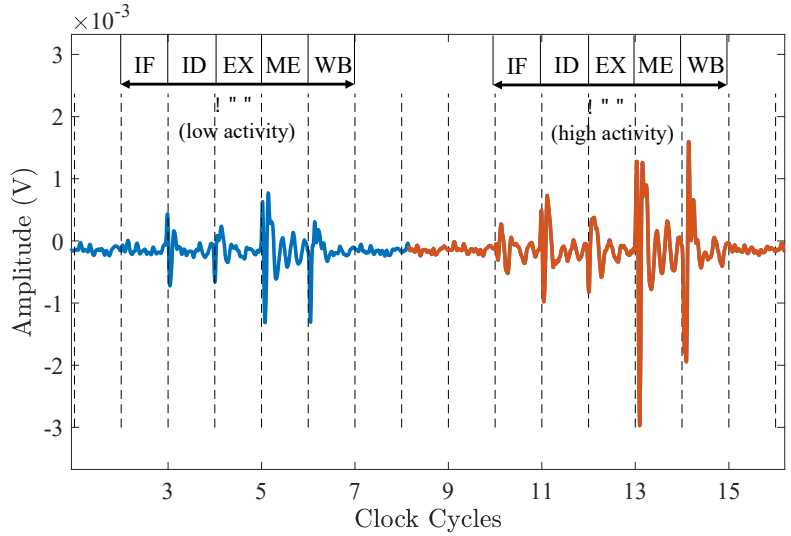
UCLA Samueli School of Engineering

Research@UCLA

Video

- Better understanding the side-channels for modeling, detection, and fingerprinting





UCLA Samueli School of Engineering

Research@UCLA

Video

- How to establish trust between (active) chips (similar to the software counterpart)?
  - Hardware/software protocols to establish trust among different chiplets. Can we use established techniques such as ***physical*** attestation to establish trust?

UCLA Samueli School of Engineering

Research@UCLA

Video

- How to establish trust between (active) chips (similar to the software counterpart)?
  - Hardware/software protocols to establish trust among different chiplets. Can we use established techniques such as ***physical*** attestation to establish trust?
  - Are there new, previously unexplored, vulnerabilities?

UCLA Samueli School of Engineering

Contact Information

Video

Building the next-generation secure heterogenous systems.

Email: nsehat@ucla.edu

Twitter: @SehatNader

UCLA Samueli School of Engineering

Thank you sponsors!

Amkor's Differentiators

Technology

Advanced Packaging Leadership
Engineering Services
Broad Portfolio

Quality

QualityFIRST Culture
Execution
Automation

Service

Design & Test Through Drop Ship
Manufacturing Footprint
Local Sales & Support

Global Companies Rate Advantest THE BEST ATE Company 2020

Advantest receives highest ratings from customers in annual VLSIresearch Customer Satisfaction Survey.

Advantest received an overall score of 9.5 out of 10, with highest ratings in categories of:

Technical Leadership – Partnership – Uptime – Commitment – Trust in Supplier – Quality of Results – Product Performance – Recommended Supplier

"Year-after-year the company has delivered on its promise of technological excellence and it remains clear that Advantest keeps their customers' successes central to their strategy. Congratulations on celebrating 32 years of recognition for outstanding customer satisfaction."

— **Risto Puhakka**, President VLSIresearch

Technical Program Committee (TPC)

Ivor Barber
Advanced Micro Devices

Jeff Demmin
Keysight Technologies

Ira Feldman
Feldman Engineering

MEPTEC
THE NEXT GENERATION

Virtual Event Schedule

Join us for two online sessions

Wednesday	April 28, 2021	8:00 - 11:00 am PDT
Thursday	April 29, 2021	8:00 - 11:00 am PDT

Your personal Zoom link is the same for both days.
Zoom will send you a reminder before the start of each session.

MEPTEC
THE NEXT GENERATION

Speakers April 28

Saverio Fazzari
Booz Allen Hamilton

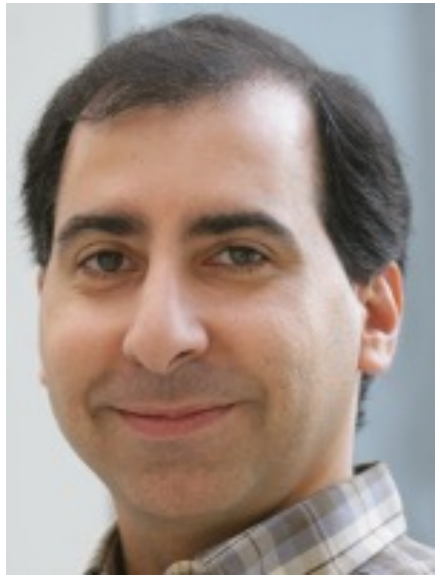
Supply Chain Challenges for Defense Systems

Sridhar Swamy & Akash Malhotra
Advanced Micro Devices

Securing Supply Chain

Nader Sehatbakhsh
University of California Los Angeles (UCLA)

Hardware and Supply Chain Security in the era of Advanced Heterogenous Integration

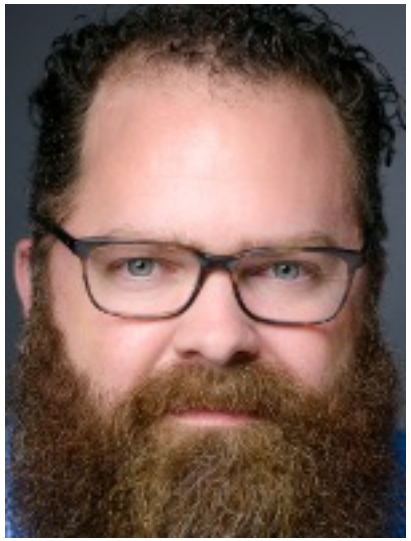


Michael Azarian
University of Maryland

Hardware Trojans and Counterfeit Microelectronics: Detection and Diagnosis

MEPTEC
THE NEXT GENERATION

Speakers April 29



Matthew Areno
Intel
Identifying Supply Chain Threats – An Honest Assessment

Ajay Sattu
Amkor Technology, Inc.
Automotive Semiconductor Unit Level Traceability

Navid Asadi
University of Florida
Physical Assurance and Inspection of Electronics

MEPTEC
THE NEXT GENERATION

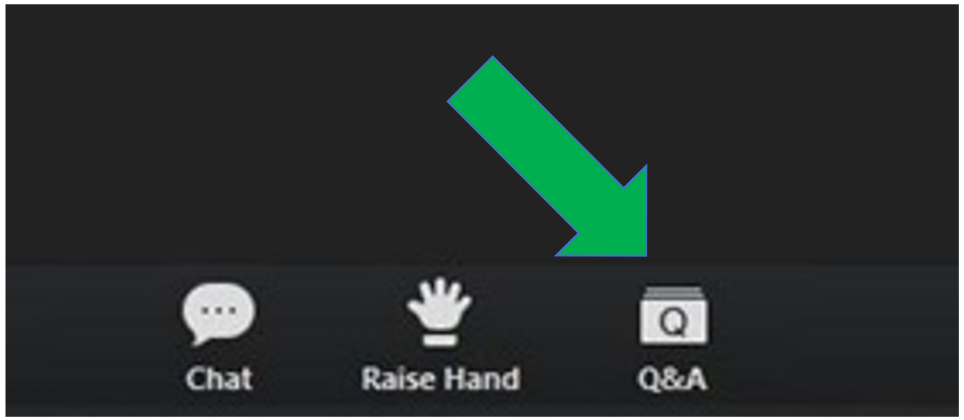
Reminders

Slides & Videos will be posted next week

http://events.meptec.org/supply-chain-security-2021 /

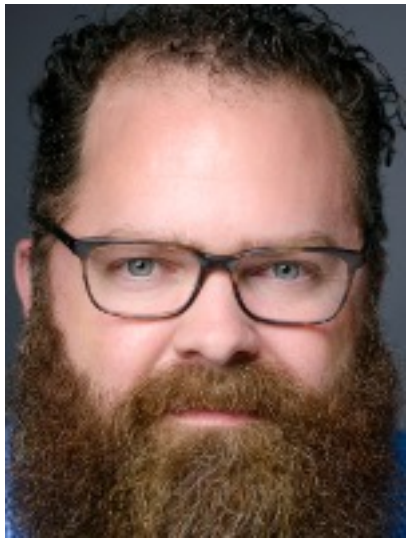
youtube.com/MEPTECpresents

Please use the Q&A window for your questions



MEPTEC
THE NEXT GENERATION

Speakers April 29



Matthew Areno
Intel
Identifying Supply Chain Threats – An Honest Assessment

Ajay Sattu
Amkor Technology, Inc.
Automotive Semiconductor Unit Level Traceability

Navid Asadi
University of Florida
Physical Assurance and Inspection of Electronics

MEPTEC
THE NEXT GENERATION

Virtual Event Schedule

Join us for two online sessions

Wednesday	April 28, 2021	8:00 - 11:00 am PDT
Thursday	April 29, 2021	8:00 - 11:00 am PDT

Your personal Zoom link is the same for both days.
Zoom will send you a reminder before the start of each session.

MEPTEC
THE NEXT GENERATION

Thank you sponsors!

Amkor's Differentiators

Technology

Advanced Packaging Leadership
Engineering Services
Broad Portfolio

Quality

QualityFIRST Culture
Execution
Automation

Service

Design & Test Through Drop Ship
Manufacturing Footprint
Local Sales & Support

Global Companies Rate Advantest THE BEST ATE Company 2020

Advantest receives highest ratings from customers in annual VLSIresearch Customer Satisfaction Survey.

Advantest received an overall score of 9.5 out of 10, with highest ratings in categories of:

Technical Leadership – Partnership – Uptime – Commitment – Trust in Supplier – Quality of Results – Product Performance – Recommended Supplier

"Year-after-year the company has delivered on its promise of technological excellence and it remains clear that Advantest keeps their customers' successes central to their strategy. Congratulations on celebrating 32 years of recognition for outstanding customer satisfaction."

— **Risto Puhakka**, President VLSIresearch

COPYRIGHT NOTICE

The content of this presentation is the work and opinion of the author(s) and is reproduced here as presented at the **Supply Chain Security Workshop** (April 28 & 29, 2021).

MEPTEC
THE NEXT GENERATION

www.meptec.org

COPYRIGHT NOTICE

www.meptec.org

MEPTEC
THE NEXT GENERATION