Supply Chain Security Workshop

April 28 & 29, 2021

MEPTEC
THE NEXT GENERATION

www.meptec.org

Identifying Supply Chain Threats — An Honest Assessment

Matthew C Areno, PhD

Principal Engineer

Security Assurance and Cryptography Lead

Intel Security Architecture and Engineering

Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

AGENDA

- Who's this guy?
- Where are we with supply chain security?
- How do I assessment my risk to supply chain attacks?
- What resources are available today to help?

WHO AM I?

- Began career at Sandia National Labs doing nation-state level, red teaming activities.
  - Focused on reverse engineering and vulnerability exploitation work against embedded systems
- Worked for Raytheon SI-Gov/Cyber Security Innovations group.
  - SME on PRoT technologies for COTS equipment
  - Graduate of Raytheon and US Navy anti-tamper courses
- Now working at Intel as the lead for the Security Assurance and Cryptography team.
  - Authored internal and external Intel documents for supply chain threat models
  - Assisting in the development of supply chain specification for ISO and USG

SUPPLY CHAIN IN THE NEWS

December 2013, Target suffered a data breach exposing 40 million customer debit and credit cards. The source of the breach was a 3rd party heating and air conditioning company with VPN credentials to Target's network.

In 2014, ForcePoint discovered malicious modules included in AutoCAD files. It is believed that the responsible party is very sophisticated and primarily interested in industrial espionage. As of 2018, over 40 unique variants of the malicious module have been discovered.

December 2020, Reuter's reported on a supply chain attack against SolarWinds, a major US information technology firm. Through a number of hacks and malware, attackers were able to compromise build and update servers to transmit malicious binaries to SolarWinds customers.

STATE OF SUPPLY CHAIN SECURITY

- "The harsh reality is that the state of our software supply chain is mediocre at best, partially due to the overwhelming complexity of the software supply chain itself."
  - *Liz Miller, VP and Principal Analyst at Constellation*[1]
- "Supply chain attacks are increasingly popular with attackers since they can access the information of larger organizations or multiple organizations through a single, third-party vendor."
  - *– Identity Theft Resource Center, 2020 Data Breach Report*[2]
- CrowdStrike reports[3] about 2/3 of respondents think their organization still has work to do to be prepared to defend against supply chain attacks.
  - Only 1/3 see supply chain attacks as concerning for their organizations over the next 12 months.

LET'S LEVEL SET

- Intel Compute Lifecycle Assurance[4] (CLA) initiative identifies four primary stages of product lifecycle:
  1. Build
  2. Transfer
  3. Operate
  4. Retire
- What standards and efforts exist today are primarily focused on Transfer and Operate phases, with little education or definition on the Build phase.
- In this presentation, we'll focus on the Build phase and how it can be assessed.

ASSESSING SUPPLY CHAIN RISK

- Determining your risk of attack and how to mitigate them is a four step, constantly recurring process:
  1. Establish the lifecycle
  2. Identify the threats
  3. Determine your mitigations
  4. Invest, invest, invest

- BE HONEST ABOUT YOUR ASSESSMENT!!!

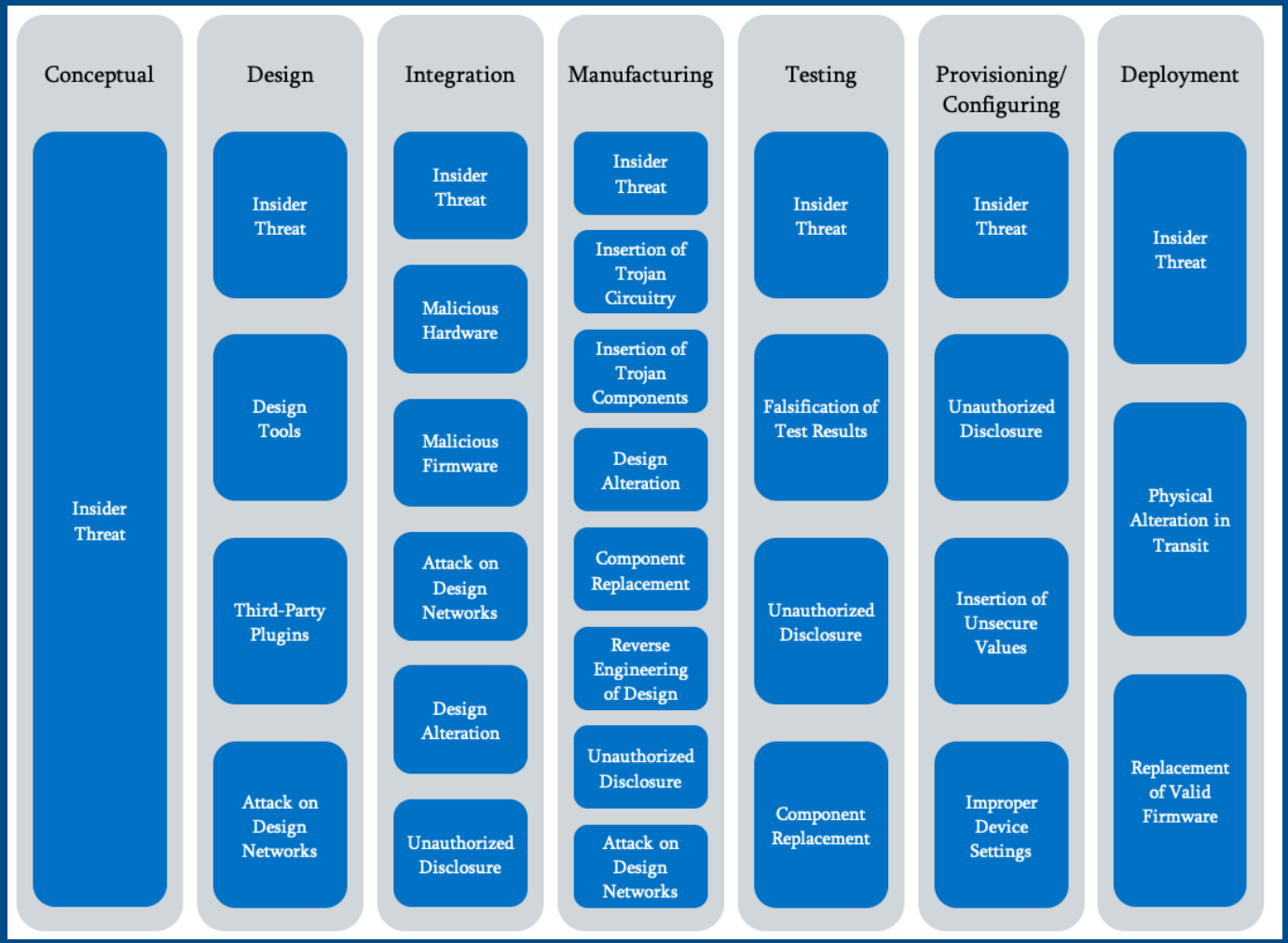
ESTABLISH THE LIFECYCLE

- Supply chains can be vulnerable across the entire lifecycle of the product.
- No single consistent lifecycle definition across Industry.
- The Build stage of the CLA has its own stages, requiring a recursive dive into each stage.
- This results in a multi-level structure of threats, starting from a Concept stage all the way to the Deployment stage.

IDENTIFYING THE THREATS

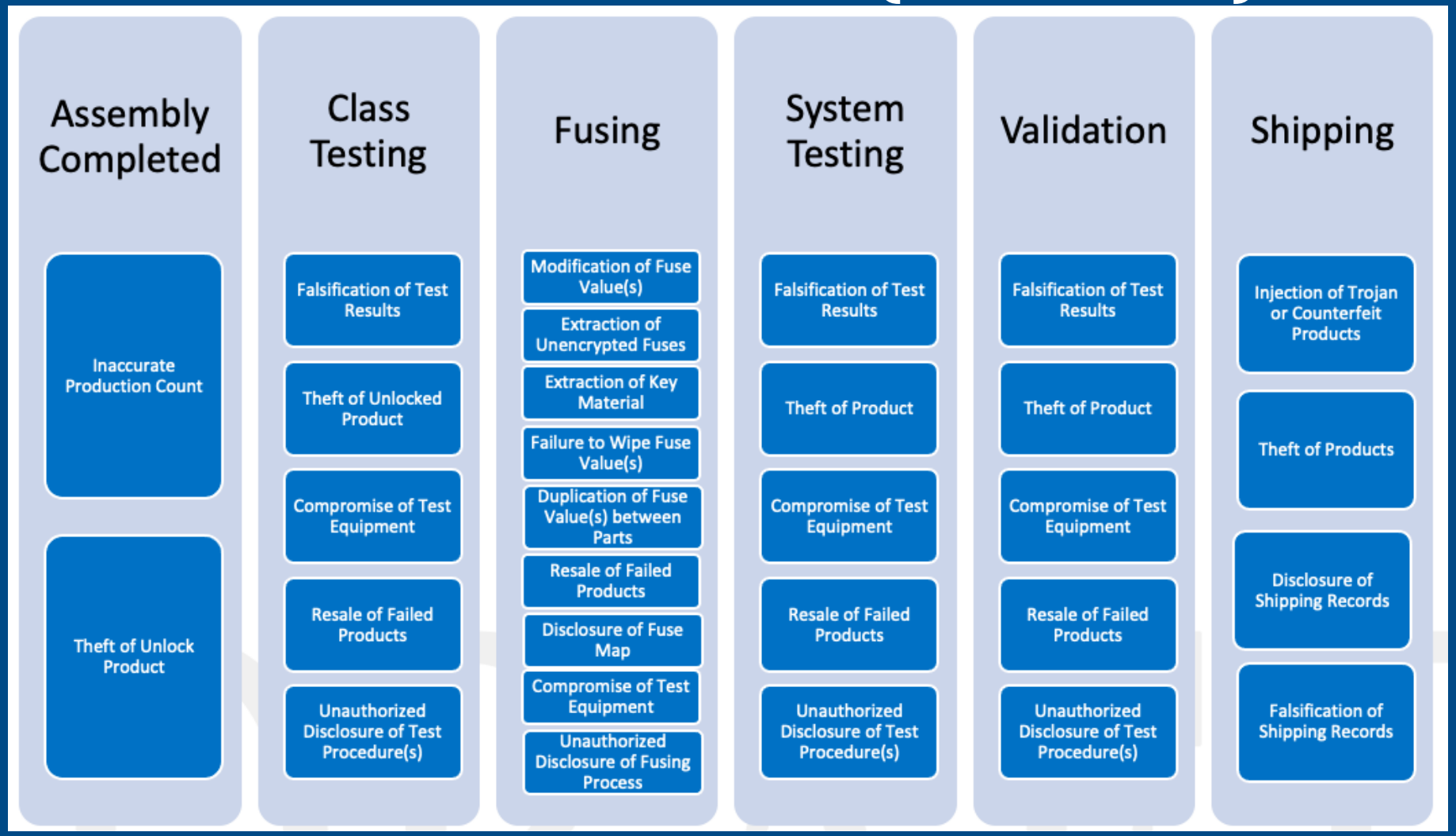
- No existing, single source of supply chain threats.
- Manufacturing is a multi-stage, multi-tier process with no single very few “sole-source” products.
- Threats affect every manufacturer and supplier, with attackers focusing on the weakest links.
- Currently a very manual process with limited amounts of automation at various stages (although it is getting better!)
- Despite differences between manufacturer processes, the threats are actually fairly standard.

IC SUPPLY CHAIN THREATS (10K FT VIEW)

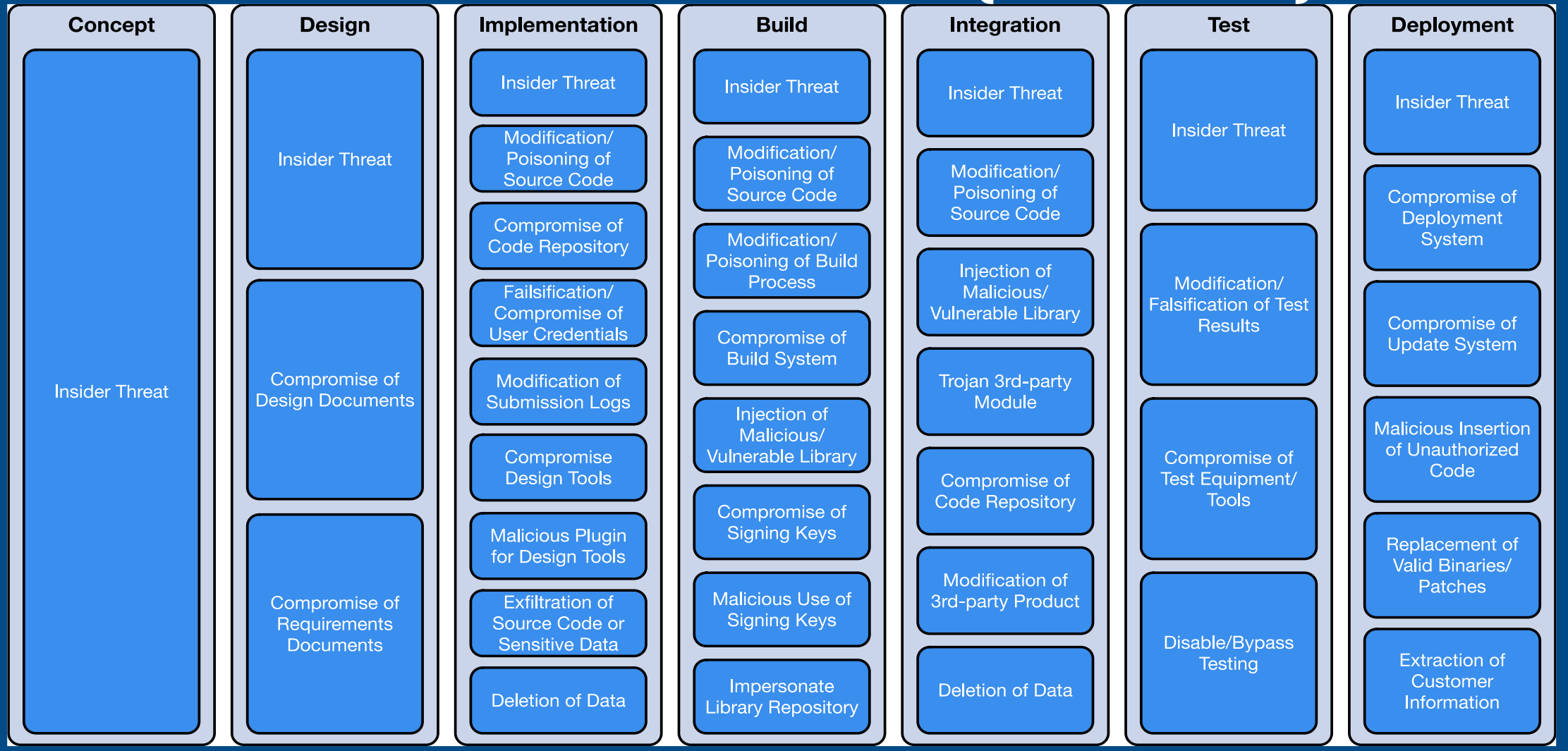


https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/supply-chain-threats-v1.pdf

KEEP DRILLING DOWN (1K FT VIEW)



SW SUPPLY CHAIN THREATS (10K FT VIEW)



DETERMINING YOUR MITIGATIONS

- Create a list of your mitigations and overlay it with the attacks.
- Now that you have the threats and mitigations identified, assess how you are doing.
  - Do I have a mitigation for this attack?
  - Is it a complete or partial mitigation?
- Identify the gaps and determine what is necessary to move your mitigations from
  - no -> partial
  - no -> complete
  - partial -> complete.
- Most mitigations have a negative impact in some aspect of your company, so consult your employees!

INVEST, INVEST, INVEST

- Create a strategy for investment.
  - As with most things in supply chain, no single formula for determining priorities.
- Suggested criteria for consideration:
  - Risk to your company (Low, Medium, High)
  - Impact to your customers (Minimal, Moderate, Huge)
  - Likelihood of exploit (Low, Likely, Certain)
  - Cost of partial and complete mitigation ($, $$, $$$)
- Sequence of invest is non-deterministic as it is, fortunately or unfortunately, often driven by current events.

SUGGESTIONS ON INVESTMENT

- Look for the low-hanging fruit or “best bang for your buck” opportunities.
- Establish timeline for tackling larger investment mitigations.
- Be transparent with your investments and your strategy.
- Plan for uncertainty, i.e. be flexible!

GET INVOLVED

- Practice transparency and push for transparency
  - Encourage your suppliers to share more information about their supply chains
  - Prepare to share more about your own supply chain
  - For ideas, check out Intel's Compute Lifecycle Assurance effort
- Support efforts in standards bodies
  - Global Semiconductor Alliance Security WG – Trusted Supply Chain
  - Trusted Computing Group – Supply Chain Security Working Group
  - ISO/IEC SC27 WG4 TR6114 – "Security assurance throughout the life cycle"
  - SEMI – Initiative for traceability starting at wafter test with unique chip identity
  - NIST – Cybersecurity framework and best practices in supply chain risk management
  - IIC – Industrial IoT Security Framework
  - NIST NCCOE – Supply Chain Assurance
  - Accelera – Security Assurance for Electronic Design Integration (SA-EDI)
- Engage on policy and US Government efforts
  - NIST working to update 800-161 on supply chain risk management practices
  - DHS releasing information on supplier engagement practices through its supply chain risk management task force
  - Understand provisions in Executive Orders from Presidents Trump and Biden on supply chain
  - Understand compliance requirements associated with Section 889 from FY19 NDAA

CONCLUSION

- Supply Chain attacks are not going away; if anything, they'll get worse!
- We must do more and we must be honest with ourselves about what needs to be done.
- Establish the lifecycle, identify the threats, determine your mitigations, and invest, invest, invest!

REFERENCES

1. https://scceu.org/solarwinds-what-are-supply-chain-attacks-and-how-to-avoid-them/
2. https://notified.idtheftcenter.org/s/2020-data-breach-report?utm_source=web&utm_medium=sitewidenotice&utm_campaign=2020DBRReport
3. https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf
4. https://www.intel.com/content/www/us/en/security/compute-lifecycle-assurance.html
5. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/supply-chain-threats-v1.pdf

Thank You!!

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

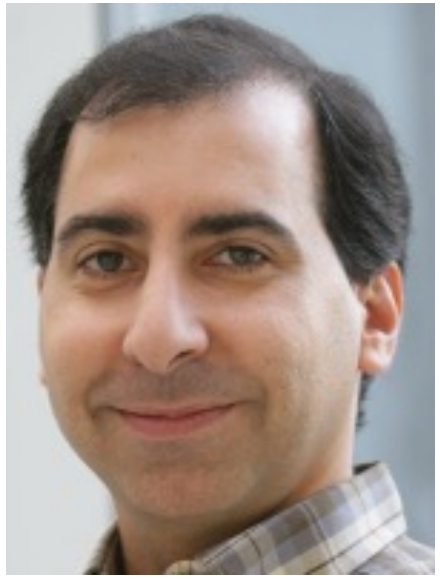
Supply Chain Challenges for Defense Systems

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

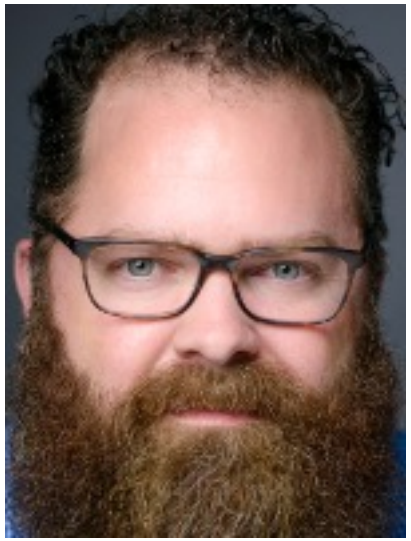


Michael Azarian
University of Maryland

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

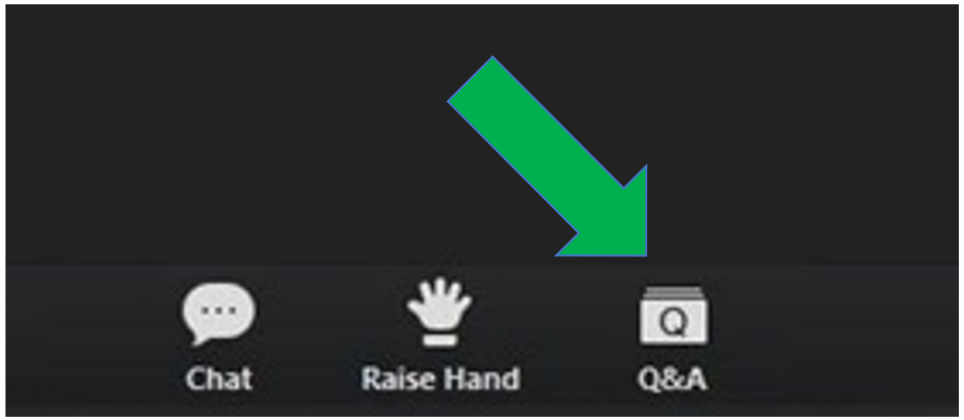
Reminders

Slides & Videos will be posted next week

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

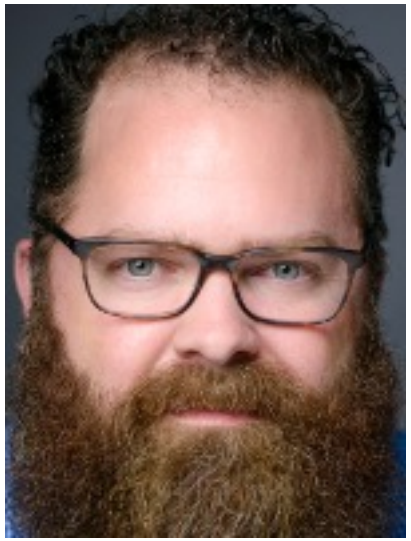
youtube.com/MEPTECpresents

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