Today’s session will be recorded.

An archive of today’s talk will be available at: www.sercuarc.org/serc-talks/ as well as on the SERC YouTube channel.

Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.

If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.

Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.
The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, ASD(R&E), nor the SERC.

No Warranty. This Stevens Institute of Technology Material is furnished on an “as-is” basis. Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.
How Can We Systems Engineer Trust into Increasingly Autonomous Cyber-Physical Systems?

5 February 2020

Dr. Joseph Mitola III, Chief Technologist
Aerospace Sciences and Engineering (ASE) Division
ENSCO, Inc., Cocoa Beach, Florida
Agenda

- Motivation: Autonomous Cyberphysical Systems
- Hardware-software Foundations of Trust
- Counter-cultural COTS Dataflow Computing Zeroizes Network Attack Surfaces
- Systems Engineering
  - Challenges
  - Enhancing SE processes
  - Opportunities
Self-Driving Tanks, Machine Guns and Spacecraft (Theirs and Ours)

The Adversaries that are selling these weapons online are bringing Autonomy to Weapons in EW-Cyber Contested Environments.
Autonomy in EW-Cyber (CEMA)
Land-Sea-Air-Space-Cyberspace
Advanced Persistent Threat (APT)

FireEye APTs
Symantec, IBM
Palo Alto Code 42
Threat Intelligence

Stuxnet 2007

Programmable Logic Controller
Software Layering Exponentiates Cyber Attack Surfaces

7 Layers

APT

APT

APT

APT

APT

APT

10^7 Attack Surfaces

Operating System (OS)

Virtual Machine (VM)

SandBox

C, C++ Libraries, DLLs

App Languages: Java, Java Virtual Machine (JVM)

Scripting Languages

Perl, Python, Ruby

Protocols: HTTP

Browser: HTML, PHP, JavaScript

CPU/RAM

APT

DevOps

$$$

$10^7$

© 2020 ENSCO
Hardware Cyber Hardening

- **Wireless**
  - RF
  - RX
  - TX
  - FPGA

- **Wired**
  - Network
  - I/O DMA
  - CPU Registers /NoC
  - Intel TXT

- **Compute**
  - ROM/RAM
  - Cache
  - Crypto/Signatures

- **Storage**
  - Hard Drive

**Hardware Roots of Trust**

- Trusted Platform Module (TPM)
- TPM
Hardware Cyber Hardening

- Wireless: RF, RX, TX, FPGA
- Wired: Network, I/O, DMA, CPU Registers /NoC, Intel TXT, TPM
- Compute: DoD Chips, ROM/RAM, Cache, Crypto/Signatures
- Storage: Hard Drive

Hardware Roots of Trust: TCORE
Protecting COTS CPUs is Impossible

\textit{COTS von Neumann Stored-program CPU Architecture Cannot Be Guaranteed Safe()}

\begin{align*}
\text{Unsafe}(\{R\}) & \quad \text{Mon}(1) & \quad \text{Mon}(2) & \quad \ldots & \quad \text{Mon}(j) & \quad \text{Mon}(j+1) \\
\text{Safe}(\{R\}) & \quad \ldots
\end{align*}

\begin{align*}
\text{Power Set of } \text{Safe}(\{R\}) & \text{ is not decidable } \Rightarrow \text{Monitor}(R_j) \text{ can never be complete} \\
\text{Hackers [Erickson] “Bits are bits”}
\end{align*}
Pure Dataflow Pipeline Safe Alternative

**COTS/GOTS**

150 Watts, 100k CVE

**“Pure” Dataflow**

40 Watts, 0 CVE
Pure Dataflow Web Server 2014-2020

Web Server Machine

www.hackprooftechnologies.com

Xilinx FPGA (1/4 of chip)
Pure Dataflow COTS
Trustworthy Autonomous Systems

Value Chain

- Script
- GUI, DB
- Libraries
- OS
- CPU

Networked FPGA-based Microservices

Time
Trustworthy Autonomous Systems

Networking Autonomous Swarms
5G vs. 4G

- E2E Latency (ms)
- Device Density (Devices/Km²)
- Data Rate (Speed - Mbps)
- E2E Reliability (%)
- Capacity (Mbps/m²)
- Availability (%)
- Broadband Connectivity (Peak demand - Gbit/s)
- Mobility (Km/h)
5G Network Slicing

Enhanced Mobile Broad Band (eMBB)

Ultra Reliable Low Latency Comms (uRLLC)

Massive Machine-Type Comms (mMTC)

Physical Infrastructure
Autonomy Enablers from 5G

Source: Financial Times, December 12, 2018
Orchestrating 5G for Trustworthy Autonomous System of Systems

TN – Transport Networks  CN-Core Network; VINNI – Virtual Network  
DCO Defensive Cyber Operations;  MEC – Mobile Edge Computing
Systems Engineering Challenges

- Pure Dataflow (No CPU/OS) is Counter-cultural
  - CPUs are OK at design time, but not at runtime
  - DirectStream data plane / control plane / antitamper
  - DoD could support the nascent dataflow ecosystem

- Systems Engineers Should “Require”
  - Entity Self-awareness
  - Domain specifications for domain-based
  - Hardware-based Machine DNA
  - Hardware self-checking

- Systems Engineer Multisensory Awareness
  - Dead reckoning, visual awareness, GPS
    - Makes GPS spoofing much more difficult
  - Apply to mission-critical requirements
Systems Engineering for Trustworthy Autonomy

- Functions
  - Enduring ("requirements")
  - Self-aware, user-aware, social animal

- Component Specifications
  - Hardware: sub-Turing, self sensing & limiting
  - Software: dataflow cross-compilers

- Design Rules
  - Allocate functions to components
  - Require clarity (IETF)
  - Require practical modularity
    - “Structured Design” ↔ Microservices
Systems Engineering Opportunities

- Demonstrate Trustworthy Autonomous Systems
  - Autonomous cell phone would
    - Know who you are and what you do
    - Assist you with mobility, banking, fitness, health
    - *Would NOT tell the network* or anybody else
  - Define OODA-loop architectures for $\Sigma$ AI/ML
- Global collaboration?
- SERC Research Directions?
  - Discussion
SERC Research Review 2020: Save-the-Date

NEW LOCATION:
NATIONAL PRESS CLUB
529 14TH ST. NW, 13TH FLOOR
WASHINGTON, DC 20045

SAVE THE DATE
17-18 NOVEMBER

SERC 2020
SPONSOR RESEARCH REVIEW

For more information, contact Monica Brito: mbrito@stevens.edu
Visit our website for more information: https://sercuarc.org/research-reviews/
UPCOMING TALKS:
“Autonomy and Trust for Cyber-Physical Systems” Series

April 1, 2020 | 2:00 PM ET
Dr. Jeff Voas, Computer Scientist, US National Institute of Standards and Technology (NIST); co-founder of Cigital, now part of Synopsys

June 3, 2020 | 2:00 PM ET
Dr. Martin Törngren, Professor, Department of Machine Design (MMK), KTH Royal Institute of Technology

CONTACT
Editor-in-Chief: Dr. Barry Boehm, University of Southern California – boehm@usc.edu
Webinar Coordinator: Ms. Mimi Marcus, Stevens Institute of Technology – mmarcus@stevens.edu

Please visit the SERC Talks page to register and for more information and updates.
Thank you for joining us!

Please check back on the SERC website for today’s recording and future SERC Talks information.

Subscribe and follow SERC on our social channels: