RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-W05

Embedded Systems Security: Building a More Secure Device

Randall Brooks, CISSP, CSSLP
Engineering Fellow
Raytheon
@randallsbrooks

#RSAC

Raytheon

Objectives

- What are common embedded systems?
- What issues do they face?
- Recommendations for securing embedded systems

Poll

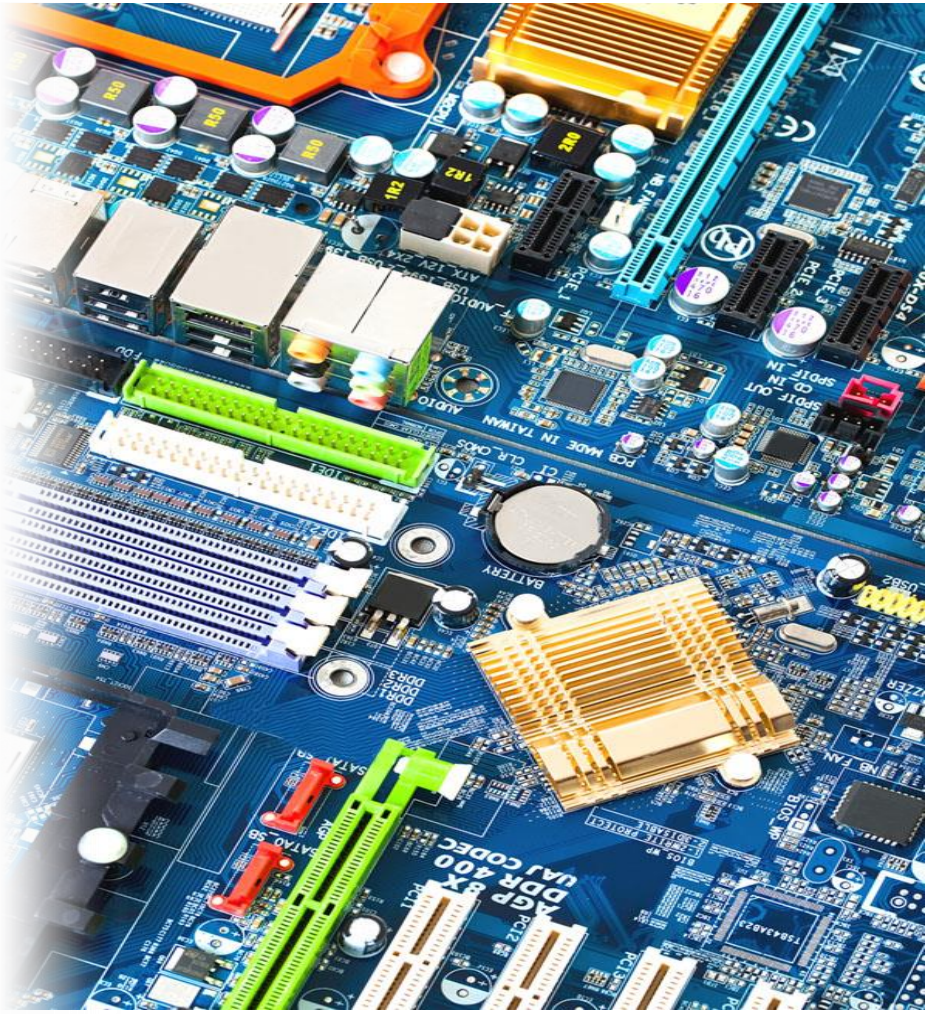
- Which operating system is your software most commonly developed for?
- Which language is your software most commonly developed for?
- Which hardware does your system run on?
- What are your thoughts on the following statement: My system is standalone, therefore many Cybersecurity or Software Assurance (SwA) requirements do not apply?
- What do you perceive as the biggest threats to your embedded system's security?
- Given the rise of IoT, do you feel IoT and its issues are related to your embedded system's security issues?

Results (Predicted)

- OS: Green Hills and VxWorks
- Language: C++
- Hardware: PPC (SoC)
- Standalone: Systems are not actually standalone
- Threats: Supply chain, physical access
- IoT Threats: IoT mirror without legacy issues

Results (Actual)

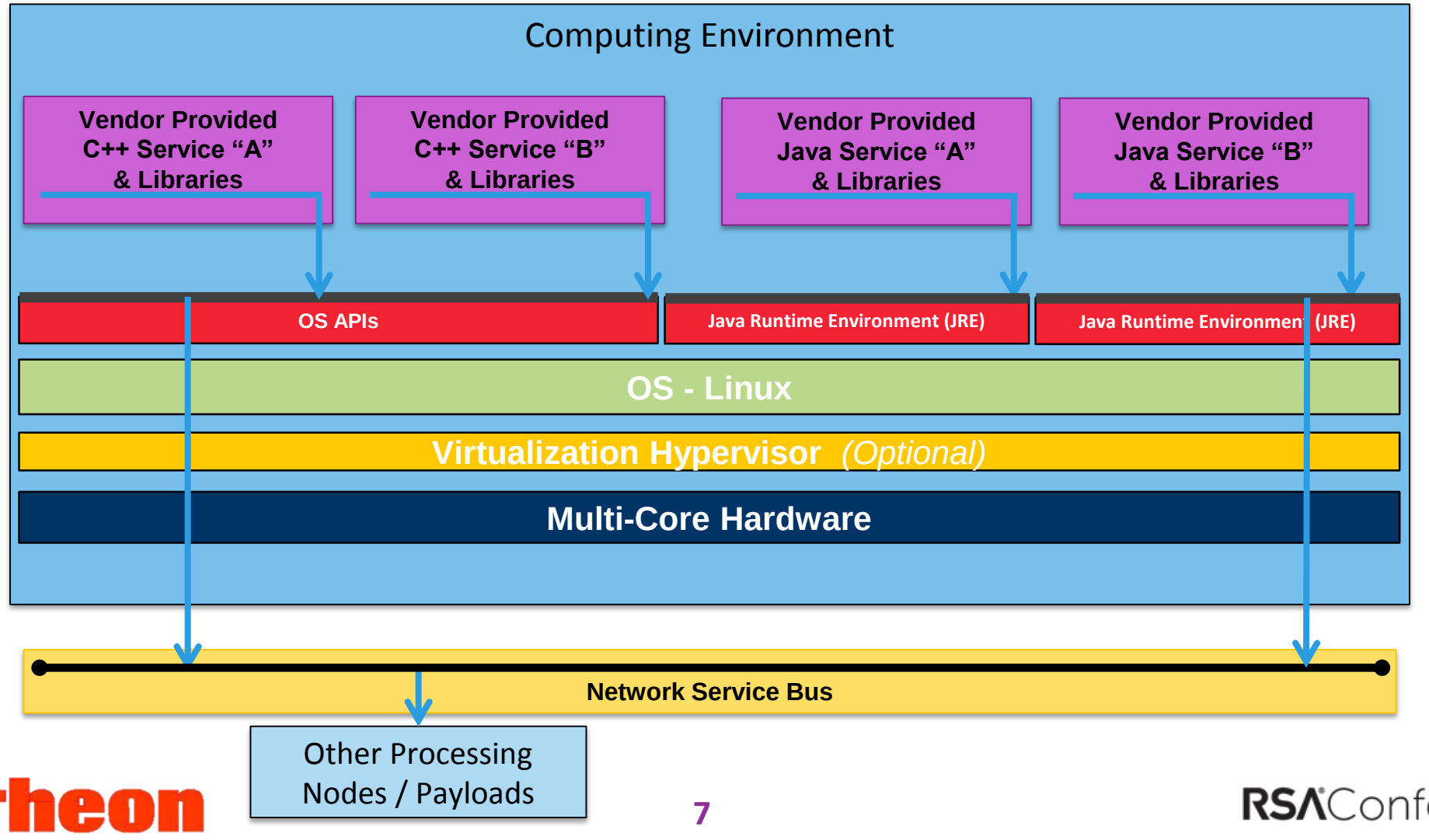
- OS: Large increase in the use of Linux and even Windows
- Language: C/C++, Java, and even Ada
- Hardware: x86 (SoC)
- Standalone: Systems are not actually standalone
- Threats: Supply chain, physical access, reverse engineering
- IoT Threats: IoT mirror without legacy issues



Audience Poll

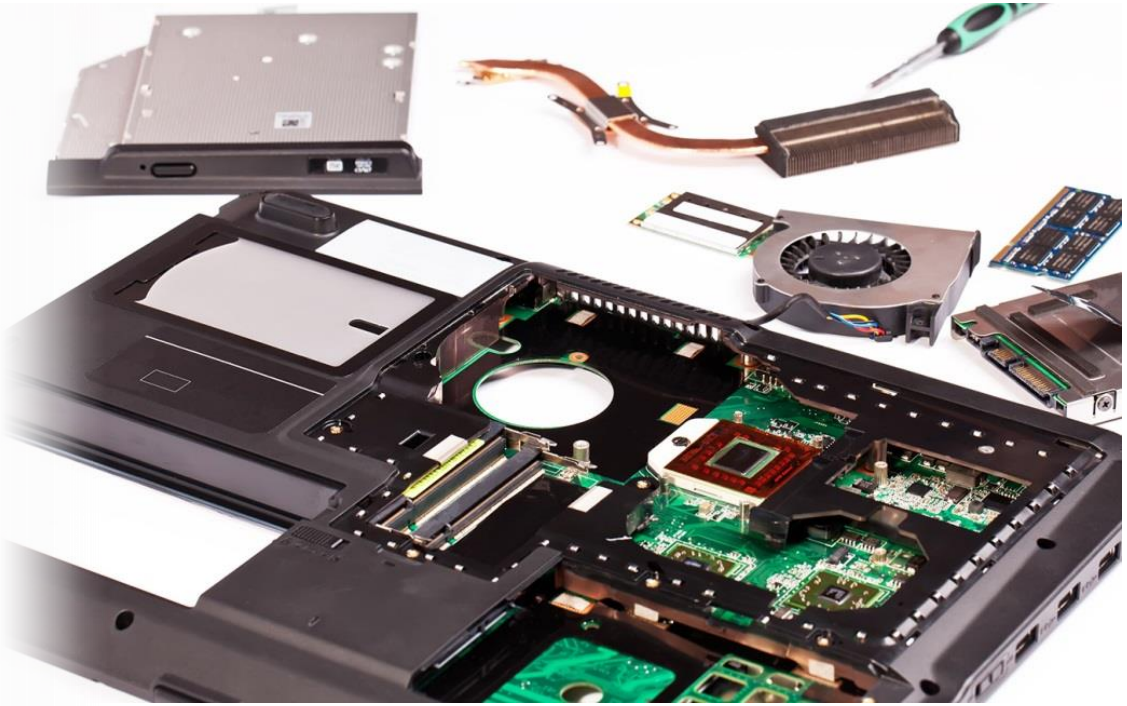
- Which operating systems do you see or use?
- Other languages?
- Which about hardware?
  - MIPS?
  - ARM?

Example Embedded Computing Environment



Traditional Embedded System Issues

- Storage components
- Processing power
- Battery life
- Time-to-market
- Overall cost



Functionality, Security, and Cost: Pick Two

The Troublesome 12 Embedded Systems Cybersecurity Threats

Supply Chain/Counterfeit Parts	Legacy Systems	Cascading Faults
Physical Access	Patch update process	No Secure Configuration
Reverse Engineering	Custom protocols	Design Mistakes
Network Access	Custom libraries	Humans

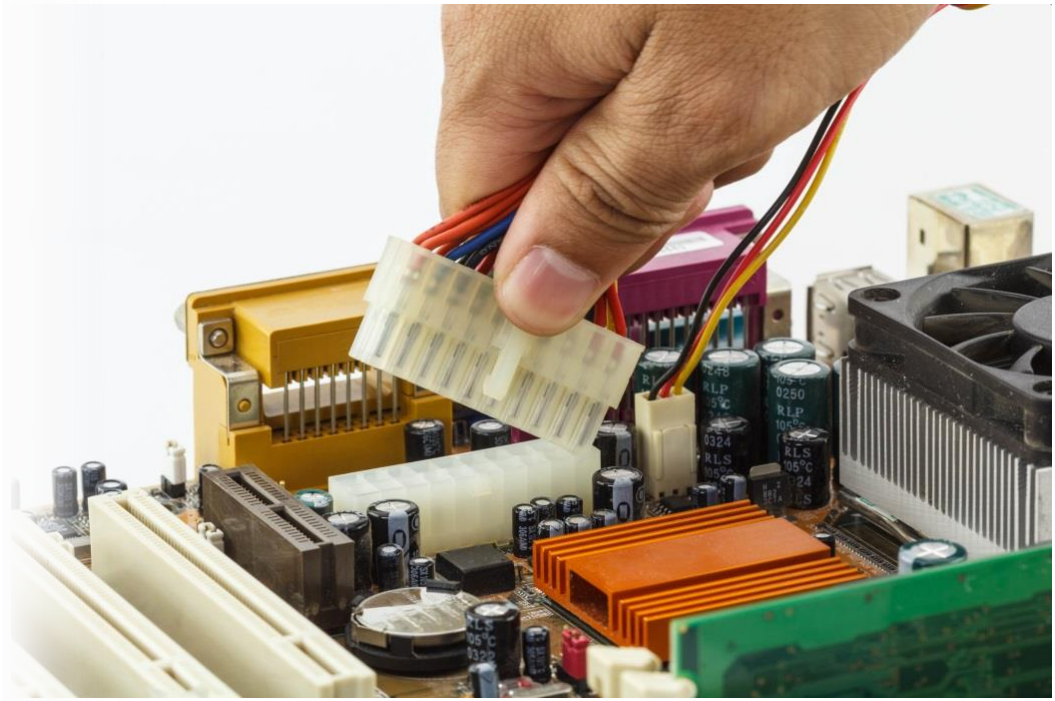
0x0c

Threat: Supply Chain/Counterfeit Parts

- Make vs. buy
- Quality vs. counterfeiting vs. malicious alteration
  - Vendor tracking database
- ASICS, FPGAs, and microprocessors
  - Destructive and non-destructive analysis
- Information storage in volatile memory and permanent storage
- Nano tagging

Threat: Physical Access

- Malicious access
- Maintenance connections
- Maintenance equipment



Game Over?

Threat: Reverse Engineering

- Intellectual Property (IP) access
  - System Integrity
- Disassembly
- Black box testing
  - Static Analysis Security Testing (SAST) of binaries
  - Dynamic
  - System Probing

Threat: Network Access

- Standalone systems internetworked
- Unprotected processes
- Remote access
- Radio Frequency (RF) manipulation

Threat: Legacy Systems

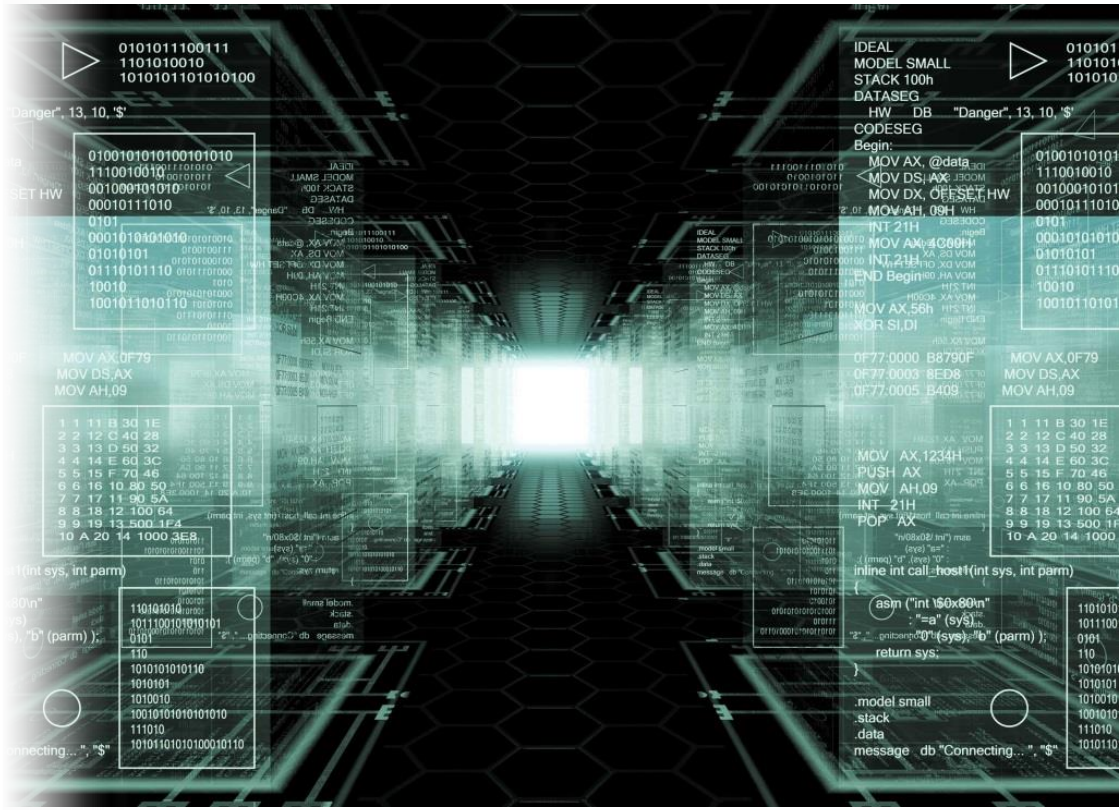
- System interaction
- Least common security measure
- Loss of technical knowledge

Threat: Patch Update Process

- None
  - Systems are permanent and not updated
- Unauthenticated
  - No digital signature on software/firmware
- Invalid
  - No integrity
- No fail secure

Threat: Custom Protocols

- Legacy
- No authentication
- Variable size
- Non-standard or multiple version support

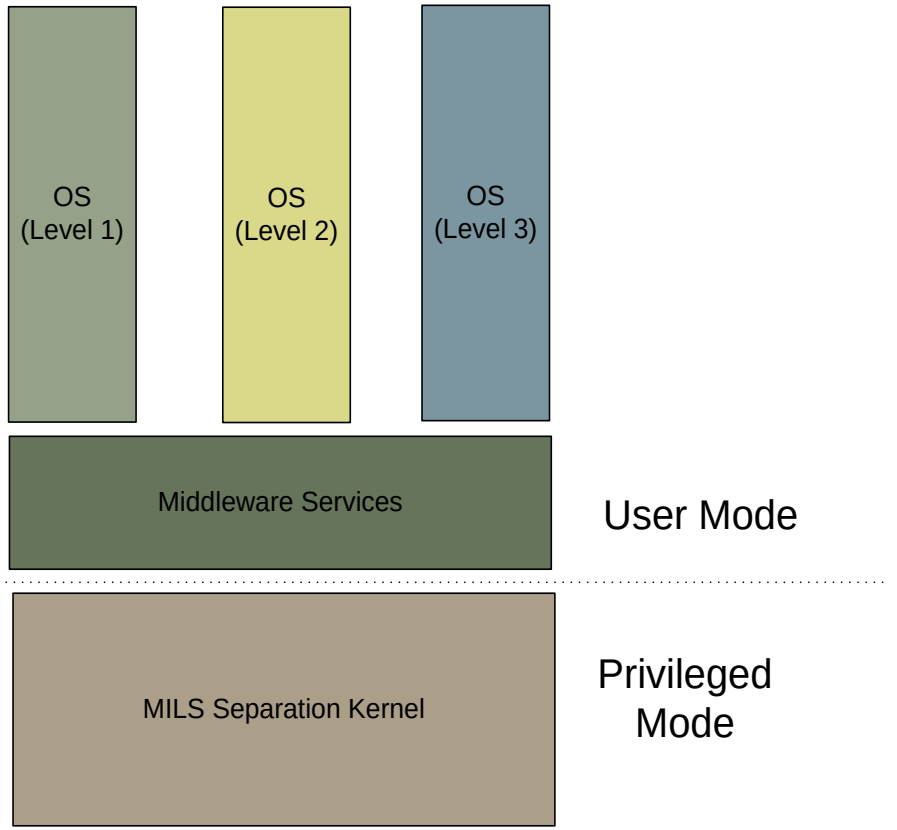


Threat: Custom Libraries

- Common functions
- Extended
- Malicious library

Threat: Cascading Faults

- Information flow – authentication and integrity for end-to-end protection of information between partitions
- Data isolation – confidentiality of data
- Periods processing – protect against covert channels
- Damage limitation – protection from a failure in one partition will not cascade to another partition.



Separation kernels keep execution separate

Threat: No Secure Configuration

- Tampered configuration
- Not secure by default
- Shared passwords across collection's embedded systems

Threat: Design Issues

- Hard-coded credentials
- Weak or missing authentication
- Improper segregation of sensitive and non-sensitive data
- Weak, custom, or excessive use of encryption
- Debug functions left in

Threat: Humans

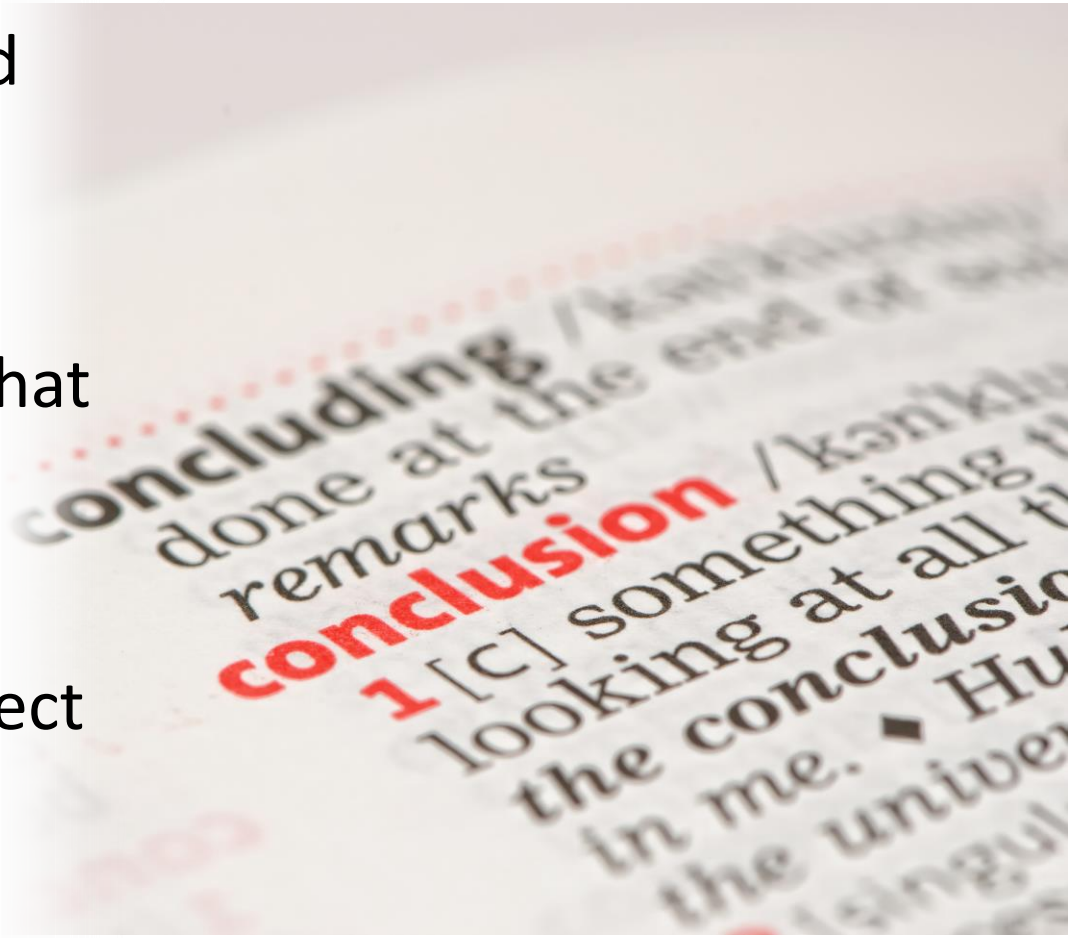
- Psychological acceptability
- Admins or users making an intentional unauthorized change or unintentional authorized change to the system.
  - Auditing, change, and control managemer
  - Training

How does this apply to IoT?

- How closely does IoT mirror these Threat?
- Does IoT have legacy issues?
  - What about the future?
- Does the key word “Internet” mean higher risk?

Conclusion

- Security functions should be built in and defend against threats within the environment.
- It is important to understand CPI and what is done to protect it.
- Host systems must maintain ultimate control over security algorithms to protect the data and prevent IP theft.



Protect Application, Execution, Data and IP

Applying What You Have Learned Part 1

Educate + Learn = Apply

As an instructor, hopefully I provided some good lessons learned.

As a student hopefully you got 2-3 key items you learned today

Take any new knowledge and apply to your development system

Let me know what you learned in the Question and Answers!

Applying What You Have Learned Part 2

- Next week you should:
  - Consider the 2-3 key items you learned from this session and start to consider where do they apply to your work?
- In the first three months following this presentation you should:
  - Do an initial Risk Assessment and consider The Troublesome 12 Embedded Systems Cybersecurity Threats
- Within six months you should:
  - Seek the advise of a 3rd party vulnerability research or assessment team
  - Train developers on Application Security/Software Assurance

Questions?

Biography

Randall Brooks is an Engineering Fellow for Raytheon Company (NYSE: RTN), representing the company within the U.S. International Committee for Information Technology Standards Cyber Security 1 (CS1) and the Cloud Security Alliance. Brooks has nearly 20 years of experience in Cybersecurity with a recognized expertise in Software Assurance (SwA) and secure development life cycles (SDLC). In addition to holding seven patents, Brooks is a CISSP, CSSLP, ISSEP, ISSAP ISSMP, and CCSK. Brooks graduated from Purdue University with a Bachelors of Science from the School of Computer Science.

E-mail: brooks@raytheon.com

Raytheon