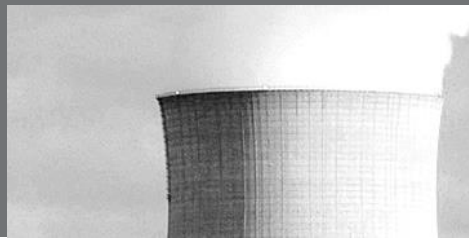
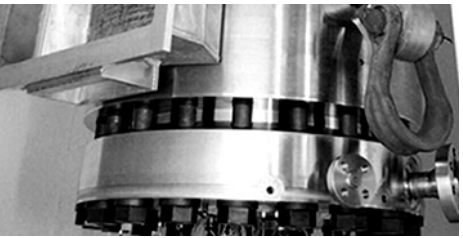
CURTISS-WRIGHT

The Convergence of Cyber Security and Anti-Tamper

David Sheets, Curtiss-Wright Defense Solutions

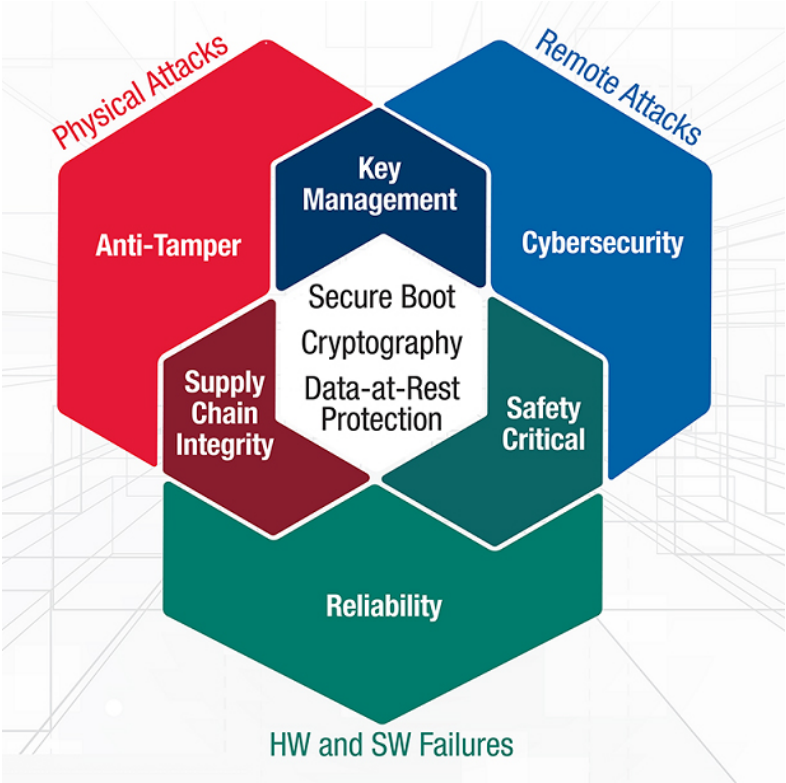




TRUSTED
PROVEN
LEADER

Types of Security

- **Cyber Security (CS)**
  - Protection against remote attacks
- **Anti-Tamper (AT)**
  - Protection against local attacks
- **Reliability**
  - Ensures HW and SW work as intended



Time Is the Enemy of Defense

- **Time allows attackers…**
  - More time to try attacks
  - Finding more bugs
  - Increases in technology
  - Older systems that aren't updated
- **Quantum computing**
  - Algorithmic obsolesces
- **What does this mean for us?**
  - Maximize resources
  - Design for upgradability
  - Find synergy where possible

Who is In Charge?

- **For AT:**
  - ATEA
  - Well defined process

Who is In Charge?...cont.

- **For CS:**
  - Independent programs
    - Much less guidance on requirements
  - The Risk Mitigation Framework (RMF)
    - Only provides a framework
    - RMF is not a silver bullet
    - Still need to look outside confines of RMF
  - Groups working to help define roles
    - Air Force: Cyber Resiliency Office for Weapons Systems

Security Requirements

- **Too constrained – limits design innovation**
- **Too loose – may not meet system needs**
- **Security disciplines**
  - Ensure appropriate mitigations
  - Still allow program cost/risk tradeoffs
- **Common security concerns**
  - Authenticity
  - Integrity
  - Confidentiality
  - Availability
- **Difficulty in finding convergence**

Impact of Classification

- **AT and CS often implemented by different groups**
- **Classification levels**
  - Can complicate interactions
  - Can stifle collaboration
  - Differences in Security Classification Guides (SCGs)

Prevalence of Open Source Tools

- Open Source prevalent in Cyber Security
- Explosive growth of concern over CS in the commercial world
- Department of Defense has concerns about use of Open Source
  - Insider Threat
  - Trojan Applications

Who Wins?

- **Disagreements between disciplines will occur**
- **AT and CS may differ in responses**
  - Continue mission?
  - Halt operation?
  - What does fail secure mean?
- **How to resolve these issues?**
  - Lack of centralized authority requires hard discussions
  - Analyze the risks
  - Get agreement between all stakeholders.
  - Discrepencies should be resolved early

Possible Synergy

- **How can you find that magical synergy that everyone is always looking for?**
- **The Good News:**
  - There are many promising areas for effective and efficient collaboration between AT and CS.

Cryptography

- **Cryptography is an integral tool for both disciplines.**
  - Share implementations between disciplines
  - Hardware-enabled cryptographic engines available
- **Design new architecture for upgradability**
- **Plan for next tech refresh**
  - Ensure refreshes enable new algorithms

Secure Boot

- **Electronic systems need to start secure**
  - Secure Boot
- **Implementation details are architecture and system specific**
- **Each discipline has their own concerns**
- **Disciplines can work together to ensure that Secure Boot is robust**
- **Ensure commercial technologies continue to grow**
  - Xilinx FPGAs
  - Intel Boot Guard
  - NXP Trust Architecture

Nature of Flaws

- **Complexity of attacks are increasing**
- **Cyber attacks are getting increasingly sophisticated**
  - *Rowhammer* – Low level DDR timing exploit
  - *Meltdown* and *Spectre* – Low level CPU pipeline exploits
  - Attacks no longer just exploiting software vulnerabilities
  - Targeting the lowest level of hardware to subvert system operation
- **Cyber Security needs to understand low level hardware**
- **Both disciplines rely on hardware**

Artificial Intelligence

- **Artificial intelligence (AI) in security**
- **Relative infancy**
- **Coming soon**
  - Systems learn their own behavior
  - Systems monitor for anomalies
- **AI can drive cross domain synergy**
  - Integration can strengthen both domains
  - Systems can learn their own environment

Safety

- **Safety shares goals with AT and CS**
  - Authenticity of hardware and software
  - Integrity of the system
- **But..**
  - Decision on actions may differ
  - Safety normally prioritizes continued operation
- **Partitioning Systems**
  - Offers integration of safety and security
  - Can introduce complexity

Upgradability

- **Most important aspect of security for most areas**
- **Difficult to securely implement at the lowest level**
- **Commercial vendors providing increasingly complex security**
- **Systems need to plan to grow with security needs**
- **Need secure methods for updating deployed firmware and software**
  - Patch known flaws
  - Defend against new attacks

Speed is Essential

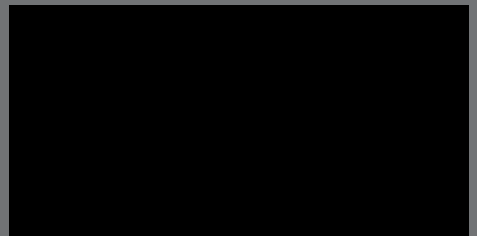
- **During an attack, time is not on the defender's side**
- **Ensure systems can be updated quickly and efficiently**
- **Where to put resources**
  - Seek the risk/cost balance in security (it's difficult!)
  - Stay up to date on the latest attacks
  - Quickly develop capabilities to mitigate attacks
  - Leverage capabilities to fulfill multiple requirements

Conclusion

- The process is difficult
- Vendors and suppliers are stepping up to provide new capabilities
- Enhance security of all DoD systems
- Security is a never-ending war
- Secure upgradability is key
- Convergence of disciplines will allow resources to go further

Thank You

For more information about system security from the COTS perspective please contact us at ds@curtisswright.com.



TRUSTED PROVEN LEADER

www.curtisswrightds.com