Introduction to COTS-based Trusted Computing

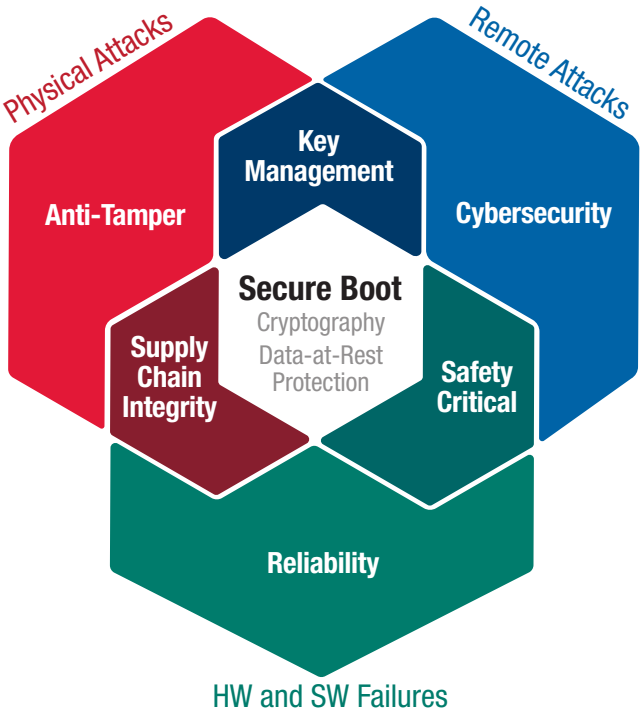
Trusted Computing: The COTS Perspective Series

Read About

Introduction to Trusted Computing
Anti-Tamper
Cybersecurity
Reliability
Supply Chain Integrity
Safety Certifiability

Introduction

This is the first of an ongoing series of papers that will address the use of open standards-based commercial-off-the-shelf (COTS) technologies to address Trusted Computing requirements in deployable embedded systems for aerospace and defense applications. First, lets define what we mean when we talk about Trusted Computing.



The Elements of Trusted Computing

Trusted Computing are those technologies and techniques that protect embedded electronics modules and integrated systems from physical and remote attacks and from hardware and software failures. Through Anti-Tamper methodologies and avionics Safety Certifiability processes, Trusted Computing also ensures that a system will only execute what is intended and nothing else. In the aerospace and defense market, solutions based on embedded hardware are frequently used in critical applications that may involve sensitive and classified information. The goal of all Trusted Computing activities is to enable the operation of these systems with complete confidence that they are secure and un-compromised. Trusted Computing also delivers confidence that

any critical data or IP will not benefit our adversaries if the hardware falls into enemy hands. Anti-Tamper defines the set of solutions to protect against Physical Attacks on the system. Cybersecurity defines those protections fielded against Remote Attacks. System Reliability results from activities designed to mitigate hardware and software failures. Approaches for providing Trusted Computing for Anti-Tamper, Cybersecurity and Reliability can intersect in various ways.

Reliability and Supply Chain Integrity

For example, Reliability, includes Supply Chain Integrity, which ensures that supplied parts and software don't introduce vulnerabilities into the system. Another important element of Supply Chain Integrity is to put into effect a Counterfeit Electronics Parts Control Plan (in accordance with the AS5553B and AS6174 Anti-Counterfeit Part Processes). The effectiveness of these efforts can have a direct effect on the Anti-Tamper portion of the overall Trusted Computing efforts, because maliciously altered or counterfeit devices can provide weak links that an adversary might exploit to intrude into a system.

Safety Certifiability for Avionics Systems

To address the increased use of manned and unmanned aircraft in domestic airspace, Safety Certifiability processes ensure that COTS hardware avionics is provably designed and developed using a process that results in a certifiable product able to meet the required DO-254 Design Assurance Level (DAL) for hardware, and DO-178C DAL level for software. By providing supporting artifact packages for these products, which otherwise can take years and millions of dollars to develop, COTS vendors are able to greatly reduce design risk and more quickly and cost-effectively enable the deployment of avionics solutions that are certified safe for use in domestic airspace.

An Ongoing Discussion About Trusted Computing

This series of papers will consider all of the elements that make up an effective Trusted Computing strategy, including Anti-Tamper technology protection, Cybersecurity data protection for software/algorithms for data-at-rest and data-in-transit, and Reliability processes for protecting the supply chain.

By their very nature, many of these topics can not be delved into with great detail and specificity. But, there are subjects, such as Cybersecurity, for which much public information can be shared. For more sensitive topics, discussions will be kept at a very high level. While it might not be possible in some cases to provide specifics, the reader will learn what questions they should be asking their COTS suppliers in order to keep up to date and informed about threats, mitigating techniques, and options. Communication between system designers and COTS designers is one of the most effective tools for ensuring that steps are being taken to develop powerful Trusted Computing solutions. To ensure that these approaches are as strong and effective as possible, COTS vendors and system integrators should as early as possible in the design stage of the program begin a conversation about what steps are available to meet Anti-Tamper, Cybersecurity and Reliability requirements. It's always more difficult to add security by backfilling than it is to build it in from the ground up.

In future papers, we will discuss such topics as data encryption, trusted/secure booting, protection of data-at-rest, protection of data-in-transit, and safety certifiability for airborne avionics systems. Trusted Computing doesn't have an end point, it's an ongoing process that evolves with new threats and new technologies. When properly undertaken, Trusted Computing enables the protection of an embedded system's data confidentiality and its operational integrity, both physical and virtual, while optimizing its availability for use in critical applications. This paper will provide a platform for shining light on known and emerging options for keeping embedded systems secure.

Author(s)

Steve Edwards
Director, Secure Embedded Solutions & Technical Fellow
Curtiss-Wright Defense Solutions

About Curtiss-Wright Defense Solutions

Curtiss-Wright has a long history of designing embedded computing products for the most demanding environments, and over a decade of experience developing Ethernet switches. Curtiss-Wright networking products are deployed in many of the world's leading military and aerospace platforms where they provide critical connectivity for sensor processing, avionics and mission systems. To support customers with challenging networking requirements, Curtiss-Wright offers a range of engineering services to support architecture, design and troubleshooting activities. For more information on CW networking products and services, contact your local CW sales representative.

Learn More

Curtiss-Wright Products

- Data at Rest Protection
- Security Enabled Curtiss-Wright SBC and DSP Products

Curtiss-Wright Case Study

- Building a Truly Trusted Computing Solution with COTS Hardware and Intel Security Capabilities

Curtiss-Wright White Papers

- The Many Faces of Trusted Computing: What You Need to Know to Protect Critical Platforms and Data
- Getting Secure, Intel-Based Solutions to Market Faster - Why the Hardware Vendor's Boot Security Implementation Is So Important
- Beyond Trusted Computing: Extending Protection Capabilities to Deliver TrustedCOTS Solutions
- Trusted Computing: The COTS Perspective Series
  1. Introduction to COTS-based Trusted Computing
  2. Trusted Boot
  3. Hardware Features for Maintaining Security During Operation
  4. Considering the Role of Hardware in Securing OS and Hypervisor Operation
  5. Application Development, Testing, and Analysis for Optimal Security
  6. Developing a Secure COTS-Based Trusted Computing System
  7. The Impact of Protecting I/O Interfaces on System Performance
  8. Decomposing System Security Requirements
  9. Establishing a Trusted Supply Chain
  10. Certification Authorities for Trusted Computing in Military and Avionics Products

© 2020 Curtiss-Wright. All rights reserved. Specifications are subject to change without notice. All trademarks are property of their respective owners. I WW148.0620