The Many Faces of Trusted Computing

What You Need to Know to Protect Critical Platforms and Data

Read About

Trusted Computing

Cybersecurity

Confidentiality

Data Integrity

Authentication

Data Availability Techniques

Non-Repudiation

Anti-Tamper Mechanisms

Trusted COTS Computing

Protection Is Paramount

The security threats that defense and aerospace systems may be exposed to before, during, and after deployment are many and varied. As a result, every system needs the right level of protection for the risks at hand to ensure that it cannot be reverse engineered or hacked into to change expected behaviors or expose sensitive information.

The threats to critical platforms and data are very real.

In 2001, a U.S. Navy spy plane was forced to make an emergency landing on Hainan Island in the South China Sea. Knowing the potential for the Chinese to access the surveillance equipment and classified signals intelligence data on the plane once it landed, the crew attempted to physically destroy classified information on the way down.

The crew dropped laptops on the floor, stomped on them, hit them against desks, bent them over seats, smashed screens, and ripped wires out of walls. They even threw a couple of laptops out of the plane's emergency hatch. But these measures would not have been sufficient to completely stop the Chinese from recovering sensitive data[1]. The crew was able to physically destroy the display terminals and controls for the signals collection equipment, but not the critical tuners and signal processors. And, while the crew was able to erase the memory on the cryptographic voice and data communications equipment onboard, they were not able to completely destroy them.

Despite the fact that the pilot and crew made considerable attempts to disable access to the equipment and classified information onboard, there was widespread criticism that their efforts did not go far enough. Some thought the pilot should have ditched the plane at sea or attempted a riskier landing in Vietnam to better protect the critical onboard assets.

Info

curtisswrightds.com

Email

ds@curtisswright.com

While there were people onboard to help mitigate risks during the 2001 flight, the increasing use of unmanned vehicles brings new security challenges. In 2011, Iran announced that it captured an American unmanned aerial vehicle (UAV) by using cyberwarfare techniques to take control of the vehicle. An Iranian engineer later explained that the Iranians had exploited a navigational weakness in the system and were able to spoof the drone's GPS with coordinates that sent it to Iran, rather than its home base in Afghanistan[2]. While some dispute the exact techniques used to capture the drone[3], it did end up in Iranian hands. And Iran has proudly stated that it successfully reverse-engineered most of the technology on the drone[4].

These are just two examples of real-world risks to critical platforms and sensitive data. Both highlight the crucial need for system integrators to trust that each solution in a system includes the right level of Trusted Computing protection and the right approach to security for the system they are building.

Know Your Terms

Today, every integrator of defense and aerospace solutions is asked to provide assurances that their solutions deliver various levels of Trusted Computing. They will refer to trust and cybersecurity and any number of other security-related features. But what exactly do these terms mean? And how can an integrator be sure that a solution provides the level of protection a particular system needs? The key is to understand the role that each security capability plays in protecting the solution and the overall system.

Cybersecurity generally refers to the software side, or the data side, of security. Cybersecurity techniques may be used to verify the authenticity of software systems to make sure they have not been compromised. For example, cybersecurity authentication techniques ensure that a computer boots from only signed and authorized boot code, the operating system kernel and drivers have not been altered, the application software is properly signed and authorized, and data has not been altered or accessed by unauthorized agents.

But software cybersecurity is just one side of the story. In many cases, security features that are implemented at the hardware level offer a greater ability to secure, or harden, the solution because they may be harder to duplicate or crack and can operate or react much faster than software solutions. For example, cryptography is often implemented at the hardware level because speed is crucial. Hardware-based security techniques may be implemented at the system level, the board level, or the chip level within the hardware.

Many security features, including most of those described in this section, incorporate protection techniques at the hardware level and at the software level. Understanding the capabilities these features provide helps in understanding the level of security that has been applied.

Confidentiality Protects Privacy

Confidentiality techniques keep information private so it is not visible to those who should not be able to see it. Confidential information is typically encrypted using complex cryptography algorithms, so even if it is intercepted, it cannot be understood. In defense and aerospace systems, confidential information may include mission information, targeting information, or algorithms and technologies, such as those used in radar systems, to identify approaching objects.

Integrity Verifies Data Has Not Been Altered

Data integrity techniques check whether data has been changed since it was last known to be valid. These techniques do not identify what data has changed, they simply indicate that the data has been altered in some way. For example, if malware was inserted into an operating system or a database, the value of the data integrity check would indicate that the software or data is not exactly the same as it was before the insertion.

Authentication Restricts Access to Data

Authentication techniques grant the right data access levels to the right people and systems based on logins, passwords, and other credentials. For example, senior officers and senior IT personnel will have access to more systems and more data than junior personnel. Authentication is related to confidentiality in a system. A senior officer's credentials must be authenticated before he or she is given access to confidential information.

Availability Ensures Access to Systems and Data

Data availability techniques ensure that data is not blocked from the systems that need it. Consider a navigation system that relies on GPS data. If the GPS data were to become unavailable, due to GPS jamming or other methods, it would be a critical problem for many different types of deployed systems.

Techniques that ensure data availability increase the resiliency of systems so the correct data continues to flow despite malicious efforts to stop it. The internet provides a good example. Even if the internet connection between two cities was severed, data would continue to be available to people in both cities because there are so many alternate data paths available.

Non-Repudiation Ensures Transactions Are Valid

Non-repudiation techniques ensure that the systems on both sides of data exchanges consider the transaction to be valid. For example, if an adversary tried to spoof a GPS signal to make it look like a vehicle was in a different location than it actually was, the system would recognize that the GPS information was not coming from the correct satellite.

Anti-Tamper Mechanisms Protect Against Physical Attacks

Anti-tamper techniques typically safeguard technology should an adversary gain physical access to it. There are three aspects to anti-tamper mechanisms:

- **Protect:** Protection mechanisms might involve completely enclosing a board or a system so it cannot be physically accessed.
- **Detect:** Detection mechanisms provide notifications if someone is trying to physically access the hardware or the software, for example by removing a cover or inserting a probe.
- **Respond:** Response mechanisms ensure that the technology cannot be accessed even if physical access is detected. These techniques may include self-destruction or automatically erasing the data in the system or on the board.

Understand Key Concepts

Along with understanding the security capabilities that comprise Trusted Computing, it's important to understand what Trusted Computing means as a concept and how it relates to Trusted Commercial Off-The-Shelf (TCOTS) computing.

Trusted Computing Requires a Layered Approach to Security

Trusted Computing is a broad concept that encompasses different security techniques and technologies. As a result, the phrase is used in many different ways. Trusted Computing ensures:

- That the computer will consistently behave in expected ways, and that the computer hardware and software will enforce those behaviors
- That hardware and software architectures, designs, tools, and algorithms will ensure the validity and confidentiality of computing results

The second definition best captures the breadth of Trusted Computing. It reflects the fact that every element in a solution plays a role in ensuring that the system behaves in the way it is expected to behave and that the data is always accurate and available and provided to only authorized recipients. Essentially, security must be implemented at every layer of each solution to create a system that can be fully trusted.

No single layer of security is ever foolproof. Each solution must be built so that if one layer of security is broken or compromised, there are other layers that continue providing protection. Picture slices of Swiss cheese layered on top of one another. Each slice may have some holes, but by layering the slices, holes can be covered by other layers with non-overlapping holes.

Or, picture an onion, where the core is still protected even if one or more outer layers is peeled away. With this approach, one compromised layer doesn't compromise the entire solution.

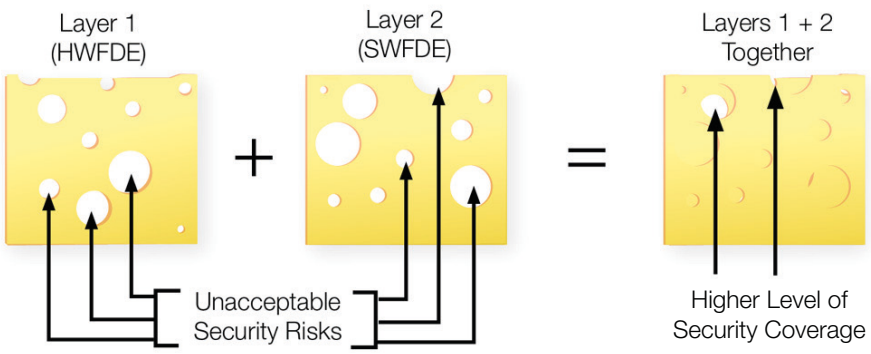

Figure 1: The Layered Approach to Trusted Computing

Within Trusted Computing, various techniques are used to help protect each layer and enable the capabilities described in the previous section. It's the combination of techniques and capabilities that enables the security at each layer. For example, hash techniques may be used to identify data that has been changed to protect the integrity of the data, but the hash does not protect the confidentiality of the data. Instead, cryptography techniques that scramble data are needed to protect confidentiality whenever data is transmitted.

In many cases, a vendor will not, or cannot, describe exactly how data is being protected. For example, there are anti-jamming techniques that counter GPS signal jamming attempts, but revealing how that is done would put important information into the hands of adversaries.

Trusted COTS Computing Extends Beyond Trusted Computing

Most system integrators are familiar with the many benefits of incorporating cost-effective COTS solutions that have been ruggedized to meet defense and aerospace demands. Trusted COTS computing is exactly what it sounds like — Trusted Computing for COTS solutions. However, Trusted COTS computing goes above and beyond basic Trusted Computing to enhance the value that COTS solutions can provide in a secure system.

There are three main aspects to Trusted COTS computing:

- **Technology protection** safeguards how computing tasks are executed. It may incorporate hardware capabilities, software algorithms, and operations that protect functionality, such as how the algorithm in a radar application works.
- **Data protection** safeguards software algorithms, data-at-rest, and data in motion. It ensures that, for example, when data is sent from one system to another, it is not compromised.
- **Process protection** safeguards the supply chain. A trusted supply chain ensures there are no compromises made in terms of the components themselves or how they are handled. For example, process protection includes anti-counterfeiting mitigations to ensure that only valid, uncompromised components are included in the COTS solution.

The third aspect of Trusted COTS computing — process protection — is one that is often forgotten when vendors are discussing security measures. But it is very important because it incorporates protection mechanisms even before the hardware components are assembled into a solution.

This broader approach to security is what takes Trusted COTS computing beyond basic Trusted Computing. With Trusted COTS computing solutions, system integrators can take advantage of an end-to-end, layered approach to security that combines commercially available security capabilities extended with the vendor's security expertise. System integrators can further extend security measures by incorporating their own expertise or program-specific security extensions into the system.

Partner With a Security Expert

By performing a comprehensive security assessment, system integrators can determine what aspects of a system are important to secure and how best to ensure that an entire system is secure.

Discussing security requirements with a Trusted COTS security expert, such as Curtiss-Wright, helps integrators assess the threats for a particular system. For example, integrators will have a better understanding of whether some or all hardware, some or all software, or only specific algorithms or data need to be protected. And they will understand whether data requires logical protection, network protection, or perhaps physical protection. Once threats are identified and analyzed, potential mitigation strategies can be evaluated with the Trusted COTS partner.

Curtiss-Wright has a deep understanding of security requirements in the defense and aerospace industries and builds Trusted Computing capabilities into many of its solutions. Curtiss-Wright also extends its security practices well beyond those of most COTS vendors to provide complete Trusted COTS computing solutions.

Security measures at Curtiss-Wright start with the supply chain, following AS5553-compliant and -auditable practices to ensure that components and technologies are obtained from trusted sources. Measures extend to include software and hardware technologies that are designed to protect critical program information from all forms of logical and physical threats. And they involve working with customers and partners to tailor products to meet the ever-changing and unique security requirements of programs destined for domestic and foreign operations. All Curtiss-Wright products adhere to globally acknowledged quality standards, such as AS9100, to ensure that processes and products can be trusted to meet the highest quality standards.

The Data Transport System (DTS1) file server reflects Curtiss-Wright's leadership and expertise in Trusted COTS computing. This tiny, ruggedized file server was the industry's first COTS data storage system to meet the requirements for the National Security Agency's (NSA's) Commercial Solutions for Classified (CSfC) two-layer encryption approach for secure data-at-rest.

Author

Aaron Frank, BaSC,

Senior Product Manager,

Curtiss-Wright Defense Solutions

In addition to secure storage solutions, Curtiss-Wright brings Trusted COTS computing capabilities to its range of processor cards. While the specific implementations may differ based on the processor type, most contemporary Curtiss-Wright single board computers (SBCs), digital signal processors (DSPs), and FPGA modules incorporate various hardware and software methods to provide confidentiality, integrity, and the other Trusted Computing capabilities described in this paper.

Conclusion

It is critical to understand the role that each security capability - such as authentication, non-repudiation, and anti-tamper mechanisms - plays in protecting any defense solution and system. Trusted Computing employs various techniques to enable these capabilities, but Trusted Computing for COTS solutions goes even further to provide technology, data and process protection. Working with an experienced partner like Curtiss-Wright helps system integrators evaluate their system security needs and determine the best method of implementation to ensure their entire system is secure.

To learn more about Trusted Computing and Curtiss-Wright's security expertise, look out for our next white paper in this series where we'll take a closer look at the Trusted Computing capabilities that can be implemented on Intel-based processor cards.

Learn more

Technology: Trusted Computing

White Paper: COTS Encryption for Data at Rest

White Paper: Trusted COTS: Leading the Way to Secure Systems

References

1. https://theintercept.com/2017/04/10/snowden-documents-reveal-scope-of-secrets-exposed-to-china-in-2001-spy-plane-incident/

2. https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

3. https://www.wired.com/2011/12/iran-drone-hack-gps/

4. http://www.cnn.com/2014/05/12/world/meast/iran-u-s-drone-copy/index.html