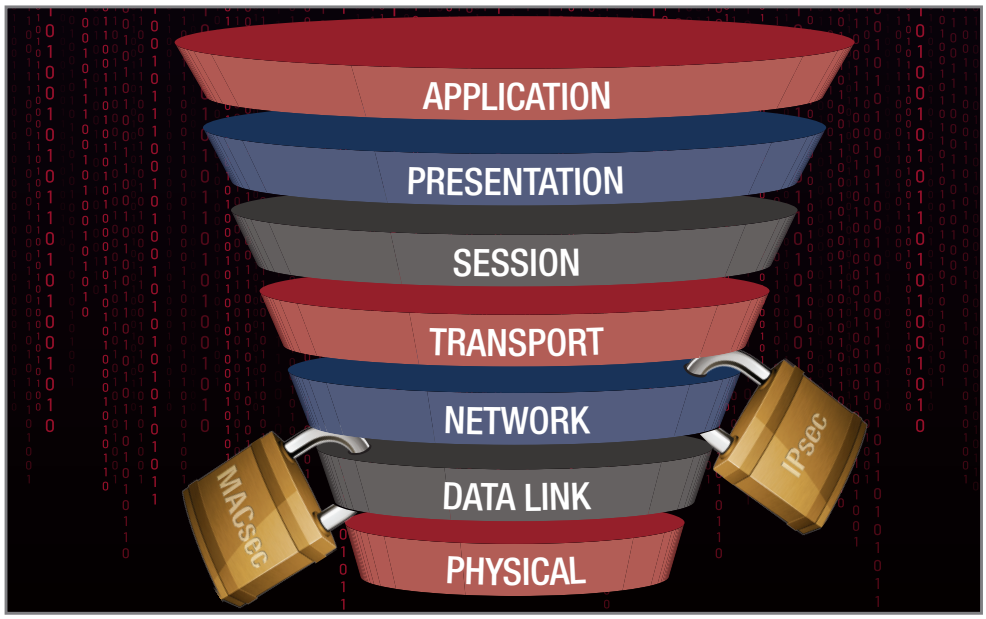
Trends in Network Cybersecurity

Trusted Computing: The COTS Perspective Series

Read About

Introduction

In our previous white paper, Optimizing Cybersecurity on Today's Connected Military and Commercial Aircraft, we emphasized the importance of safeguarding data and establishing a secure communication link. Here, we highlight network security in the embedded space, increasingly a target of scrutiny these days. In a constantly evolving threat environment, where new attacks arrive virtually every day, system architects must design networks to be as secure as possible. That requires a constant review process in order to enable the adaptation, modification, and updates needed to keep your system safe.



MACsec and IPsec are two standards that provide authentication and encryption on different network layers.

Network security involves providing protections against all devices that are connected, or might potentially have access, to the network. In this area, embedded architectures are in the process of catching up to the sophistication of security in enterprise networks. In the enterprise environment, where there has always been the risk of an unauthorized person connecting on a port in an office or conference room, the need to lock down the network is well understood. One the other hand, embedded systems haven't always had this exposure, making their control simpler.

The Need for More Secure Embedded Networks

In the past, embedded networks such as those installed on aircraft would have been tightly controlled, with no network ports exposed for physical access. Today, embedded networks are expanding to connect more devices and between systems that previously would not have been connected. In a commercial aviation environment, Ethernet might be available at every seat of the aircraft and Wi-Fi might be provided for entertainment.

As more devices become connected to the embedded network, the "surface area" that needs to be protected increases significantly. Adding to the challenge of implementing network security is the growing trend towards converged networks. Instead of a single purpose network that only connects within a single-function system, faster links can now transport data from a variety of disparate systems over the same network, requiring less cabling. More systems sharing the network increases the potential for contention, but also increases the security challenge - more endpoints means more potential sources of threats. Converged networking is also increasingly common in military embedded systems. The good news is that there's growing awareness of what's needed to secure an embedded network, and many of the important tools are familiar and readily available.

One tool for securing the network is "white-listing" - limiting access to trusted devices. This could be as simple as specifying that each port only allows traffic from a specific, known MAC address. While simple to implement, this approach is also relatively easy to defeat, because MAC addresses can be changed and spoofed. Trusting a device just because it has the right address turns out not to be a very robust security solution.

A more advanced technique for protecting against unknown users involves the use of 802.1x, an IEEE standard for port-based Network Access Control (PNAC). Using 802.1x, the network can authenticate an endpoint that's connected to a port using a cryptographic exchange before it's allowed to use the port. With this approach, instead of trusting a device on the basis of its MAC address, trust is based on a certificate or other credentials. Since gaining access to an 802.1x requires software on all endpoints that will connect to a switch, this approach requires a whole-system solution where both the network and embedded devices must support the feature.

Layers of Encryption

Another challenge for providing network security on embedded systems results from upgrade cycles. If a security layer needs to be added to a system, but only one of the devices on the network has that layer, a weak link will be introduced into the overall system, unless all other devices on the network are also provided with that layer of security.

While hard-coding and 802.1x enable control over what devices can access the network, MACsec and IPsec are tools that use encryption to protect data on the move and prevent someone from snooping that data. IPsec is an end-to-end protocol that was originally used for VPNs that connect from one office to another office over an untrusted network. In comparison, MACsec provides more of a local approach, as it's intended to only secure a point-to-point connection.

Both IPsec and MACsec provide ways of encrypting data that travels over the network. In addition, both techniques also provide a capability for authentication by validating keys when connections are established. The two standards differ in how much of the data in the Ethernet frame is encrypted. For example, IPsec also supports both tunneling and transport modes that offer tradeoffs between overhead and the amount of data that is encrypted. Apart from IPsec and MACsec, there are also encryption standards that can be implemented at the application level, such as

Transport Layer Security (TLS). These require less support from the network infrastructure, but generally require more processor overhead and encrypt even less of the Ethernet frame because they exist at the highest layers of the network stack.

Today, we are more frequently seeing IPsec used within local networks, such as airborne networks that are contained entirely within an aircraft. This protects against data being intercepted by other devices on the network. It also provides protection if the switches in the network are compromised.

Because they need to encrypt network traffic at high data rates, it's important to select network equipment and endpoints that provide sufficient performance. MACsec encryption is typically implemented in hardware and is built into the PHY devices that provide the link-layer connections. IPsec encryption can be performed in software on general-purpose CPUs, but some degree of hardware acceleration is often needed for it to perform at full network line-rate. Ensuring that endpoints and network equipment can support encryption at the required data rates is critical when selecting commercial off-the-shelf (COTS) hardware.

Standards can also change over time, so it is important to ensure that appropriate versions of a standard are used to meet overall system requirements. For example, earlier implementations of MACsec only supported AES 128-bit encryption keys, while AES 256-bit encryption was added to later versions of the standard. It is also important to ensure that all portions of the network support the appropriate level of security.

Building an Integrated Network Security System

When it comes to implementing network security in embedded systems, a major challenge can be finding people with the required expertise. There are many highly trained networking professionals trained in protocols and architectures, but most are familiar with enterprise IT. Engineers with experience in designing rugged and reliable embedded systems may not be up to date on the latest networking technologies. The intersection of people who understand both networking and embedded systems is small, but growing. What's helping that intersection grow is the Internet of Things (IoT) phenomenon, which is taking all manner of embedded devices that were traditionally stand-alone appliances, and connecting them to networks.

While system designers are more frequently asking for network security solutions, their specific requirements are often still vague. For embedded defense application security requirements, we are in the early days. Security isn't something you can just buy from a vendor as though it's a standard feature of the product. Instead, security needs to be implemented across all products in the system and integrated within a high-level architecture. System integrators need to either perform the architecture work themselves, or hire experts to do it for them, to ensure that their security solution is cohesive from end-to-end. To be fully effective, network security must be thought out and addressed from the very beginning of the system development process when the architecture is first defined. To design effective network security, it's wise to first reach out to your vendors' network security experts at the very beginning of the project.

Additionally, take into consideration that network security doesn't end with architecture, or the initial implementation. Network security is an ongoing process that needs to be revisited on a regular basis in order to protect against new threats. Patches to address vulnerabilities and new countermeasures will likely need to be designed into each iteration of the system, at every software upgrade and every time that a new device gets added to the network.

Looking ahead, even some fundamental tools we rely on to secure networks may need to change. Today, most of the underlying cryptography used to protect networks is based on asymmetric, or public key, cryptography. As the design of quantum computers improves and they start to come online, there will likely be a need to reexamine the use of some of the underlying cryptographic primitives on which network security designers currently depend.

Author(s)

Andrew McCoubrey
Senior Product Manager
Curtiss-Wright Defense Solutions

David Sheets
Senior Principal Security Architect
Curtiss-Wright Defense Solutions

Conclusion

Network security is a complex and evolving challenge. Fortunately, for those building embedded systems, solutions are being continually developed to address emerging threats and challenges. Leveraging the latest commercial technology and employing people with the required expertise in the field of both networking and embedded systems are key to ensuring that connected embedded systems are secure, today and in the future.

Learn More

Curtiss-Wright Products

- Curtiss-Wright TrustedCOTS™

Curtiss-Wright White Papers

- Latency: Understanding Delays in Embedded Networks
- Copper or Fiber for Military & Aerospace Networks?
- 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
  11. International Certification Authorities for Trusted Computing
  12. Optimizing Cybersecurity on Today's Connected Aircraft
  13. Trends in Network Cybersecurity