
www.pipelinepub.com
Volume 19, Issue 9

# Overcoming the Knowledge Gap to Enhance Your Cybersecurity Measures

By: Dennis Mattoon

Whether in the enterprise or the consumer space, trusted computing should form the backbone of your networks to ensure digital connectivity is safe and secure. Standards are essential to establish this, comprising specifications, guidance, and software developed by internationally recognised bodies such as the Trusted Computing Group (TCG). By implementing these standards, users can rest assured any component found within a computer network can be reliably verified—keeping their network safe from malicious activity.

When it comes to security, organizations often focus primarily on device, network, and data security. These are all relevant areas to address, but one area often neglected is firmware security.
The number of attacks against firmware—the code responsible for device behaviour—continues to increase exponentially. If hackers gain access to the firmware, they can quickly gain complete control over the device and cause significant damage.

Attacks against consumer products such as smartwatches are commonplace, but with the growth of embedded systems and the Internet of Things (IoT), we are seeing a notable rise in attacks on firmware used in industrial settings. Through something as innocuous as a sensor, cybercriminals can gain access to critical infrastructure and create major disruption to operations. Not only are these attackers stealing sensitive data, but they can also modify the behaviour of certain technologies—for example, raising the temperature on a thermostat to ruin produce or endanger livestock. Consequently, solutions that can protect operations within the firmware and ensure routine device behaviour are of paramount importance.

# Establishing a ‘trusted’ network

As technologies continue to develop and evolve, so do the bodies that establish the standards and the pecifications they design to enhance security measures. The core concept of trusted computing has been expanded beyond personal computers to cover a wide range of technologies and concepts, from cloud computing and virtualization to data center technologies, automated vehicles, and supply chain security. The standards and specifications available to organizations continue to play a crucial role across a number of industries, especially finance, healthcare and industry, where cybersecurity may not always be the first thing on the agenda.

One of the most essential standards used in devices today is the Trusted Platform Module (TPM), a hardware-based security feature that ensures a safe environment for storing and processing private data. Over a billion devices across the world leverage a TPM to store cryptographic keys and other sensitive information while attesting to the identity of software, firmware, and other elements running on a device. Take the industrial sector as an example—a TPM establishes trust in communications between any devices and control systems found within a factory to protect the integrity of the device and its data.

# Choosing the right solution

Not every specification will fit perfectly with the devices you leverage, however. For larger devices, the TPM can help successfully defend against firmware attacks, but for smaller devices—such as tiny sensors found in vehicles or smartphones—this hardware Root-of-Trust (RoT) can often be larger than the device to which it attaches. In these circumstances, solutions like the Device Identity Composition Engine (DICE) are critical, but vendors may still require some guidance as to which RoT is most suitable for their requirements. DICE enables secure positioning of device identities, including the generation and management of device-specific keys. Through specifications like DICE, attributes that identify a device (such as manufacturer, model, and serial numbers) can be stored safely in a protected environment to reduce the risk of illicit tampering.

For resource-constrained devices like microcontroller units (MCU), device security typically relies on a combination of hardware protection for secrets and the fortification of measurements and keys used in firmware. Before solutions like DICE, the device firmware was responsible for most, if not all, security-critical operations. This was fine as long as the vendors included strong security measures within their offering, but it led to device performance being significantly affected. Implementing asymmetric keys to protect the secrets on a device can be a difficult and costly process, and if the firmware is directly processing the cryptography, then these keys must be generated before other important actions are carried out.

In the age of increasing device revolution, the DICE Protection Environment (DPE) specification instead marks an evolution of previous solutions available to vendors. An isolated secure execution environment can now be established separate from the firmware, capable of enhancing device protection for crucial processes through an additional layer of security. Critical operations—for example, the processing of cryptographical keys—are moved away from the firmware and isolated. This frees up the processor to carry out only its main functions, which increases the speed of the device and gives users the required tools to enhance their operations. DICE offers similar benefits to a

TPM, but in a solution more fitting for smaller applications.

The DPE also protects transitions between the boot layers of a device, hardening attesting environments and offering greater security for all elements within the "trust chain." This means that from "power-on reset" to the runtime state of a device, vendors can be assured of the trustworthiness of their devices.

# Implementation without the know-how

Now put yourself in the shoes of a silicon vendor for a moment. Knowing the benefits of standards and specifications is one thing, but having the technical understanding of how they work and how best to deploy them in your devices is another. When looking to use a solution like DICE for your own purposes, you have a number of options when it comes to implementation. If you're a vendor who has strong technical knowledge and fully understands your requirements, this is perfect; yet for many, the number of choices may only lead to misunderstanding and greater confusion. This could even result in errors in implementation and greater vulnerabilities for hackers to exploit, as well as interoperability concerns.

This is why standards bodies are moving towards technologies and specifications that offer increased guidance and best practices to potential implementors. With this additional support, organizations are able to reduce or eliminate the risk of implementation error and achieve greater interoperability, making products more compatible across the entire device ecosystem. Specifications, such as that DPE are no longer limited to devices with existing DICE implementations, are making these a valuable resource for both adopters of RoT hardware and those who have not yet integrated it into their own solutions.

This also means vendors are getting greater opportunities to develop and market their own DICE solutions in the form of a DICE Intellectual Property (IP) block. This provides the ability to adopt and integrate hardware security across solutions, reducing any unnecessary complexity and simplifying the adoption of RoT technologies that are so essential to device security. As a result, silicon vendors can now leverage technologies that offer enhanced security measures without having to fully understand the cryptographic elements associated with them.

# Forming the bedrock for strong security

The adoption of innovative technologies has had the unfortunate side effect of increased attacks from hackers looking to exploit systems and steal sensitive data. The growing threat of firmware attacks may quickly put an end to the burgeoning device revolution if the devices being used to increase productivity continue to be weaponized against operators.

If device vendors are to provide the required protection for devices, they must turn to organizations like the TCG and embrace the standards they create. Using the most up-to-date standards available can not only enhance the security measures found in devices, but can also provide guidance to avoid the pitfalls of a mis-implementation and enable greater interoperability across all industries.