www.pipelinepub.com
Volume 16, Issue 10

The Benefits of Trust in IoT Era

By: Thorsten Stremlau

With more than 21 billion Internet of Things (IoT) devices expected to be deployed by 2025, according to antivirus and anti-malware security specialist Norton, and with very little or no security hardware running on these devices, more must be done to create a safe and secure digital ecosystem. Where resources, budgets, and environments vary across devices, a number of security applications must be considered to ensure the whole ecosystem has access to a strong defense against the growing sophistication of attacks and threats.

As the market for IoT devices grows, the competition between manufacturers to offer the best capabilities at the cheapest price increases—carrying the dangerous risk of security being overlooked. This creates a threat climate like never before as these devices become an increasingly enticing prospect for hackers.

IoT devices often act as a bridge between the virtual and physical world, providing a rare opportunity for hackers to interact remotely and providing almost limitless opportunities for devices to be compromised. Attacks on products like home security cameras or smart fridges might seem mundane, but they put personal data at risk by allowing access. Often, this kind of targeting sees victims spied on through their own cameras. Or, their financial information can be stolen by opportunists who have simply exploited an insecure device. With this in mind, the importance of having a secure foundation for the rest of the security layers to be built on has never been more critical.

Roots of Trust: a foundation for security

When it comes to security, most of the attention goes to the most visible elements of a system, such as the operating system and the applications. However, with the growing number of threats, many organizations have begun to add firmware to their vulnerability and threat prevention models.

With action already being taken across the world, the latest Trusted Computing innovations in hardware security are essential to providing a simpler Root of Trust (RoT) foundation to build an anchor of cybersecurity protection. The RoT is a concept thatstarts a chain of trust needed to ensure devices boot with legitimate code. If the first piece of code executed has been verified as legitimate, these credentials are trusted by the execution of each subsequent piece of code.

Firmware and configuration data are security-critical components in any IoT device and must remain available and trustworthy in the face of an attack. These mechanisms must be resilient to tampering or corruption by destructive malware and built upon trust in the platform recovery support. In the event of a device being compromised, it needs a safe place to fall back to recover. In order to do this, a trusted hardware environment is needed, whether it is a Device Identifier Composition Engine (DICE) or a Trusted Platform Module (TPM).

Deeply rooted protection

With a wide range of security options on offer, TCG provides building blocks to create secure systems. In the case of a high-risk system, for example, industrial-grade discrete TPM hardware can be built in, not just into the plant's firewall but also into the control system. This will enable real-time monitoring and allow sophisticated attacks to be identified and prevented. For devices that have a lower risk profile, TPM firmware can be created that has the same set of commands but sits just above the hardware—and is therefore more cost-effective.

With the proliferation of IoT devices comes the increase in extremely small connected devices, presenting the new challenge of securing devices with very minimal space to operate within. These small devices cannot be left without security measures in place; doing so will create a weak access point for a cyberattack. However, the inclusion of a TPM chip could be impractical due to cost, space and power.

In order to address this challenge, TCG launched two complementary technology workgroups, the DICE Workgroup and the Measurement and Attestation RootS (MARS) Subgroup. MARS is responsible for delivering specifications needed to define what the tiniest TPM needs to be, so silicon vendors can integrate TPM functionality into their hardware. DICE provides an alternative for devices where inclusion of a TPM is impractical or infeasible. DICE allows silicon vendors to leverage existing hardware security functionality to enable foundational security scenarios that rely on device identity and attestation.

Along with other industry specifications and standards including NIST 800-193, TCG is ensuring trusted computing and security is within reach across the broadest range of devices, from high-end servers and storage to the smallest IoT devices.

Painting different parts of the cybersecurity picture

The TPM from Trusted Computing Group (TCG) is the standard hardware RoT, providing secure storage of boot and runtime state as well as cryptographic information such as private encryption keys. Resistant to physical attack, the TPM prevents attackers from recoding the device and accessing stored data by hiding these keys so that the data cannot be read and authorized users cannot be locked out. Combined with the technology of DICE, this provides cost-effective, foundational security for any system or component stemming from its simple and adaptable hardware requirements.

In addition to providing hardware-based identity and attestation, DICE creates a platform for data integrity, device recovery, and system updates. It does so with a layered boot architecture, leveraging Unique Device Secrets and individual fingerprints with each layer and configuration. This means that if different code is ever booted, the deviation from a trustworthy boot will be recognized and different secrets will be generated—preventing attackers from accessing any genuine data should they tamper with the device. If, however, a vulnerability did exist and disclose a secret, the code would automatically patch and re-key the device, making it possible to recover the data while preventing it from being read by an attacker.

Cyber resiliency is key to the protection of devices of all sizes. It is essential for developers to give devices the best chance of remaining safeguarded. This is accomplished through protection of updatable persistent code and configuration data and detection when vulnerabilities are not patched, or when corruption has occurred through the capability to recover reliably to a known good state, even if the platform has been compromised.

Preparing for future uncertainties

Experts agree that there is a void in IoT strategy when it comes to the protection of the resources and mechanisms of attestation. Through its collaboration with industry leaders, the Trusted Computing Group is focusing on their specific needs and use cases to ensure that the developed specifications offer the RoT required to protect critical resources and mechanisms. By doing so, the industry will have the necessary tools to efficiently participate in established trusted computing practices.

IoT device manufacturers of all sizes should review and recommit to developing and executing a sound cybersecurity strategy for all new products. Even those that feel fully prepared should engage with experts and ensure any products are protected against exploitation. As the threat landscape becomes more complex, device manufacturers should leverage Trusted Computing technologies to provide more agility and speed of deployment—to be safe in the knowledge that all layers of security are implemented to protect against the growing sophistication of the threats of the future.