How Healthy Is Your Web of Connected Devices?

By: Tom Brostrom

In recent years, the evolution of the Internet of Things (IoT) has seen an explosion in the number of devices connected to the Internet—a trend which is set to continue long into the future with the development of new applications driven by connected homes, smart cities and autonomous vehicles. Currently, there are over 25 billion IoT connected devices worldwide. This number is forecast to reach 30 billion by 2020 and over 60 billion by the end of 2025, according to Statista. This massive wave of new devices and applications, however, comes at a cost.

The new paradigms that IoT devices bring and the technologies that they enable are producing an exponential increase in machine-to-machine communications. With ever-increasing demands for connected devices, IoT opens up a whole host of new opportunities for enterprises and for the whole of society. Consequently, IoT also dramatically increases the possibility of security issues and threats. A recent study by SonicWall revealed that IoT attacks are escalating, with a 217.5 percent increase in the volume of attacks. While everyone wants to have their devices interconnected, many of the estimated 30 billion IoT devices that will be installed by 2020 will also come with easy-to-abuse security controls—or none at all.

Security should be at the forefront of the manufacturing process. As technological advances continue to develop innovative new products, services and connected devices, the technological tactics used by hackers will also mature, leaving organizations open to a multitude of new threats. It is now crucial that every device is protected and trusted; otherwise weak links can be utilized by hackers as an easy entry point. IoT manufacturers across the globe should opt for widely deployed and proven solutions to deliver on new and emerging security needs as we move toward a connected world.

A connected society

The emergence of the IoT era brings with it a multitude of security challenges. Insufficient testing, infrequent updating, insecure default configurations, and potentially persistent malware are all factors that weaken the security of a device. Devices considered secure when first purchased can quickly prove to be insecure and prone to security issues.

As society puts greater trust in things like autonomous cars, smart homes and healthcare sensors and connects them to the Internet, manufacturers need to take steps to ensure connected devices are ubiquitously secure to protect them from data breaches and hackers. Security in the IoT era shouldn’t be an afterthought: it should be an element that is carefully and thoroughly considered during every step of the manufacturing process.

With the proliferation of connected devices under IoT and the increase in cybersecurity threats, making devices secure against IoT security issues will become a key differentiator for manufacturers in the future. Many manufacturers of larger devices have chosen to include roots of trust in their designs that give devices the ability to securely and remotely attest to their health. Without this trusted computing capability, devices could harbor persistent malware without anyone—users, network peers, or service providers—being aware.

Organizations that have deployed applications based on trusted computing concepts exhibit superior capabilities in security governance, risk management and compliance. Trusted Platform Modules (TPMs) embody some of the key foundational principles of trusted computing and are basic building blocks used to provide roots of trust necessary for higher assurance. They are typically separately packaged as integrated circuits with sophisticated capabilities similar to a Hardware Security Module (HSM).

The challenges that IoT brings

As IoT adoption continues to grow, a rising number of devices are so small that the inclusion of a full TPM chip might be impractical due to factors such as cost, space and power. This begs the question: what can be done within the bounds of the IoT microcontroller to *implement* the essential commands that would otherwise reside in the TPM? *Identifying* these essential commands is also problematic in that it is desirable to be robust enough to be useful, but small enough to be palatable by device manufacturers. Arguably, most of the TPM specification's 113 commands would be unnecessary for very small IoT devices.

Another problem for IoT is that some devices are so primitive that they lack the resources to perform the big math required to produce asymmetric digital signatures needed to securely convey health assertions. While this type of signing is universally accepted, alternatives such as HMAC for weaker devices are well known but unpopular.

Achieving roots of trust

IoT microcontroller manufacturers are including crypto accelerators (e.g. AES) in some of their product offerings. Since cryptographic primitives form the basis of many TPM commands, manufacturers have unknowingly been building the core component of a TPM. All that is missing is a little extra state machine logic to drive the accelerators to form roots of trust. This notion was the inspiration for the creation of the Measurement and Attestation RootS (MARS) subgroup within the Trusted Computing Group (TCG).

MARS is looking to specify a small subset of TPM commands necessary to support measurement and attestation. Once this has been done, manufacturers can bake in their own MARS TPM with very little overhead. This will ensure that devices that typically lack a separate TPM will still be able to include the required roots of trust. In turn, this will allow trusted computing technologies to flourish in otherwise inhospitable areas.

MARS will also be working with other groups to adopt appropriate symmetric cipher, signing and hashing algorithms. MARS has already been in contact with NIST regarding their Lightweight Cryptography Standardization Process designed to identify crypto standards that are suitable for constrained devices. Their scope is Authenticated Encryption with Associated Data with optional hashing.

The future of IoT security

Experts agree that there is a void in the area of 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 drawing on their specific needs and use cases to ensure that the developed specifications offer the roots of trust 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.

Trusted Computing Group's new Measurement and Attestation RootS (MARS) Subgroup has been formed to develop specifications that will enable IoT manufacturers to build TCG-compliant chips with very little overhead for them and their customers. Through its innovative ideas and solutions, IoT manufacturers who were previously reluctant to add additional TPMs are able to implement some of the needed roots of trust directly onto the chip.

With Trusted Computing Group’s roots of trust, IoT device manufacturers can detect unauthorized changes to device firmware and configuration. This critical feature gives the ability for a remote resource provider to take the device configuration into consideration as to whether to allow access to its resources. With this model, somebody else can make a determination or access control decision based on what the device reports—and can trust the report.

By implementing existing capabilities and proven solutions today, IoT manufacturers can face the security threats of the future, no matter what they bring.