ARCHITECT'S GUIDE: IOT SECURITY

July 2015

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary and Action Items

The explosion of intelligent connected devices, or the Internet of Things (IoT), presents a massive expansion of the "attack surface" hackers can target. Some researchers predict the IoT will reach 50 billion connected devices by 2020. Many of these devices are vulnerable to attacks and the level of risk continues to rise. Failure to secure IoT systems has already led to several costly or dangerous incidents[1].

Critical strategies for architects include:

1. Assess IoT Goals and Risks
2. Manage Identity and Integrity
3. Encrypt Confidential Data
4. For Critical Systems, Use Hardware Security
5. Protect Limited Devices with Overlay Networks

[1] http://www.wired.com/2015/01/german-steel-mill-hack-destruction

Introduction

Every day, more things are connected to networks. These range from industrial machines to home appliances to vehicles and billions of sensors.

Data collected from these sensors and devices allows individuals and businesses to make better decisions and take advantage of new products and services. But, every new device that connects to a network is potentially instantly exposed to viruses, malware, and other attacks that could result in industrial espionage or safety and security issues. Proper security measures must be taken to protect against these attacks.

Compared to a typical corporate network, the IoT poses unique security challenges, including:

- An unprecedented number and variety of devices
- Many devices that lack the computing power or memory capacity to support even basic authentication and authorization
- Highly heterogeneous networks, a patchwork of operating systems and a wide variety of devices from many manufacturers
- Legacy/proprietary equipment and/or networking standards, such as SCADA (supervisory control and data acquisition) and other industrial control systems that often exist alongside traditional IT networks
- Demanding real-time applications, such as in manufacturing and automobiles and other transportation systems
- Potential safety risks that can result from denied access. Locking authorized users out of critical devices, networks and infrastructure can have serious implications
- Unattended and unmanaged devices that often are difficult or impossible to access for physical updating
- Software-only security mechanisms that are limited in their security capabilities
- Devices that likely will be in operation for decades, and might be manufactured by vendors who provide infrequent or no updates

Call to Action – What To Do Now

To deal with these formidable challenges, a carefully planned response is needed. The step-by-step process described here guides IoT architects as they define their business goals, gauge the security risks to those goals, and develop appropriate security controls to manage or reduce the risks.

Throughout this process, *consult Figures 1 and 2,* which show an example of this process.

STEP 1: Assess IoT Goals and Risks

Start by writing down the strategic goals for your IoT deployment. This is important because it will help you assess the importance of various IoT risks, and thus how much money and effort you should spend addressing each. When defining your goals, consider:

- Are you seeking greater efficiency, flexibility, insight, or control from the data you will gather from the IoT or your ability to control devices in it?
- Do you see a new business opportunity?
- Maybe you're complying with a mandate?

See Figure 1 for a sample list of goals.

Now sketch out an architecture diagram for your IoT system and annotate it to show how data and control flows through your system. As you proceed with this process, you will add security controls to this diagram to address the salient risks in your environment. *See Figure 2.*

Finally, write down the risks that could threaten your system and goals. To structure your work, group the risks under the three most critical information security properties: confidentiality, integrity, and availability. For each of these properties, write down what could happen if that property was lost.

- What would the impact be on your system and goals?
- How would your customers be affected?
- Can you estimate, even approximately, the financial loss, or the damage to your reputation or brand?

Figure 1: Goals & Risks

STEP 2: Manage Identity and Integrity

To protect against attacks on the integrity of your IoT system, you must ensure that only authorized parties are able to gain access. Furthermore, you must make sure that all the components in the system are not compromised (e.g., infected with malware). If compromise cannot be prevented, it must be promptly detected and remedied.

One powerful tool for integrity protection is the Trusted Platform Module (TPM). The TPM is a standard micro-controller that combines robust cryptographic identity with remote security management features such as remote attestation. Because the TPM is defined by open standards, designers can choose from a variety of TPM products from different vendors supported by common software.

STEP 3: Encrypt Confidential Data

Protecting confidential data with encryption may seem obvious, but care is required to do it right.

Data in transit should use end-to-end encryption so that eavesdroppers can't decrypt it. Because encryption is only as good as the keys and algorithms used, only thoroughly reviewed encryption algorithms and carefully generated keys with high entropy should be used. For long-lived systems, plan for key updates and even changes in cryptographic algorithms (known as "algorithm agility").

Stored data should be protected with encryption also. One simplifying technique commonly used in IoT is to not store data locally but always stream it to a powerful server where it can be easily encrypted. In any case, consider carefully where the encryption key will be stored. If this key is accessible to software, a software bug can accidentally disclose it and render the encryption useless. Keeping long-term keys in hardware is a better practice.

The self-encrypting drive (SED) standards from TCG (Trusted Computing Group) enable encryption to be built into drives, improving security while avoiding the overhead of software encryption and ensuring that equipment can be cleansed for reuse simply by telling the drive to change its key. As with TPM, the SED standard is available in a wide variety of interoperable products, including hard drives, solid state drives, hybrid drives and enterprise storage systems, from a variety of vendors. These drives are already in use in a number of devices, including printers, copiers and multi-function devices; point of sale systems; and digital signage.

STEP 4: For Critical Systems, Use Hardware Security and Standards

All software has bugs that can be exploited to compromise the software and the containing systems. For this reason, critical components in an IoT system should always be based on security hardware such as TPM and SED. A hardware approach helps ensure against malware and attacks that are typical in more vulnerable software, especially software in IoT environments that might not be patched or upgraded frequently. Open standards have the advantage that many eyes have reviewed the standards, searching for errors. This is why commercial-grade systems are generally based on open standards such as TPM and SED.

STEP 5: Protect Limited Devices with Overlay Networks

Many IoT systems include limited devices such as tiny, battery-operated sensors or legacy devices such as decades-old hydroelectric generators. These devices cannot be upgraded to include built-in security capabilities. However, they cannot be left unprotected on a potentially hostile network. The best way to protect such systems is to place them on an "overlay network" that insulates them from attacks and provides confidentiality and integrity protections for their traffic. TCG has developed networking standards for such overlay networks[1], consistent with other international standards in this area.

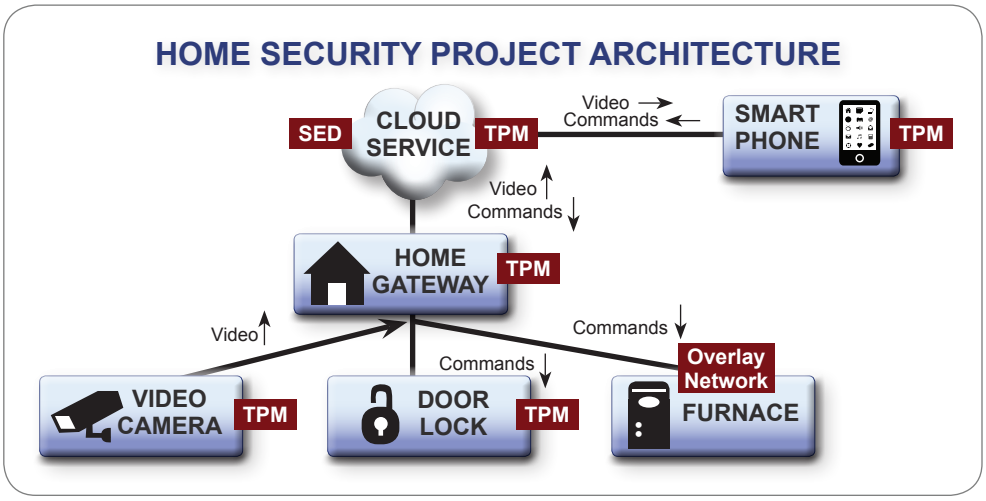

Figure 2: Project Architecture

[1] IF-MAP Metadata for ICS Security

The IoT Now and in the Future

The IoT is still in its infancy. Enterprise customers and everyday consumers are only beginning to understand its benefits, much less the security implications. Given the high level of interest in IoT, security breaches that cause financial damage, compromise personal information or even cause physical damage will inevitably arise in the next few years, resulting in disproportionate attention and financial and brand damage to those involved.

Ensuring the identity and integrity of IoT devices, as well as the security of their data storage and communications, will allow organizations and consumers to get the maximum benefit from the IoT with the least risk.

Future

TCG and its members will continue to work on implementation options for existing TCG standards and technologies. The group also will examine whether future standards that reflect the unique requirements of the IoT, including power consumption, footprint and cost, will be useful and necessary. TCG also will evaluate how it can further enable the need for automated operation of IoT systems, including automated detection of threats, prevention of infection, and responses to infected systems.

References

[IoT] Trusted Computing Group, “TCG Guidance for Securing the IoT”,
https://www.trustedcomputinggroup.org/resources/tcg_guidance_for_securing_iot

[ICS Security], Trusted Computing Group, “Architect’s Guide, ICS Security Using TNC Technology”,
https://www.trustedcomputinggroup.org/resources/architects_guide_ics_security_using_tnc_technology

[Cybersecurity], Trusted Computing Group, “Architect’s Guide, Cybersecurity”,
https://www.trustedcomputinggroup.org/resources/architects_guide_cybersecurity

[TPM] Trusted Computing Group, “Trusted Platform Module”,
https://www.trustedcomputinggroup.org/developers/trusted_platform_module

[Self-encrypting Drives] Trusted Computing Group, “Self-encrypting Drives”,
https://www.trustedcomputinggroup.org/developers/storage