TPM 2.0 AND SMART BUILDINGS

Smart buildings result from the integration of several of today's sensing, communication, power and computing technologies into an architectural structure. According to the Building Efficiency Initiative Organization, "…enabled by technology, this smart building connects the structure itself to the functions it exists to fulfill…" The organization goes on to define those as:

- Connecting building systems
- Connecting people and technology
- Connecting to the bottom line
- Connecting to the global environment
- Connecting to the smart power grid
- Connecting to an intelligent future

The good news is connectivity offers many benefits to building owners and managers as well as residents and tenants. The bad news: connectivity and the inclusion of buildings into the Internet of Things (IoT) and related data, cloud and networks opens these buildings and their data to known and emerging security/trust issues.

The Benefits

Smart buildings and building automation systems (BAS) provide a systems approach to address lighting, heating, ventilation, air conditioning systems and security in office buildings, factory buildings and even homes. Using sensing, communication, computing and power (actuator) technologies, the goal is improved and more efficient illumination, thermal comfort, air quality, sanitation (plumbing and water management) and physical security --- all resulting in increased productivity.

In a Nov. 2015 report, Zion Research projects that these desired benefits will take a global smart building market valued at $7 billion in 2014 to $36 billion by 2020. The existing portion and certainly the expanding portion should have trusted and secure connectivity.

The Security Issues

Physical security, including extensive use of cameras, RFID tracking, key cards, finger print and face recognition, motion and/or other sensors, is an integral part of smart buildings. However, cyber security issues of hacking, unauthorized entry and other security breaches that result in malicious property destruction and information as well as physical property theft are just starting to be addressed.

In addition to the vulnerability of physical security systems to network attacks, there are building control systems that have safety components - some which could risk human lives. In well thought-out applications, the safety of people is always the number one concern. Industrial control systems are no exception. They are always designed to protect people, even in a system failure, as a first priority. A few examples bring out the significance of cyber protection to prevent physical failures.

Consider the smart building's elevator system. If compromised, an attacker might intentionally or by accident cause a control failure on the elevators, resulting in a car full of people free-falling 50 floors. Interference with building heating ventilation and air conditioning (HVAC) system might result in catastrophic failure that threatens lives or closes the building (for repair) for weeks. Also, interference with a building's electrical system might cause deadly shocks or a fire. These systems are not designed to protect safety in the event of compromise by network-based attack.

Since the IoT controllers and actuators that govern some systems have safety implications and are helpless in the face of cyber-attack, it falls to the owners of those systems (the building owner in this case) to accept responsibility for the safety of the building's occupants. In addition to the tragic (and preventable) loss of life, if someone in the building dies, a lawsuit for negligence can be brought against the building owner for failure to adequately protect safety critical systems from cyber-attack.

A 2015 incident in a German steel mill provides a very real –and frightening - example. An intentional or inadvertent cyberattack made it impossible to shut off the factory's blast furnace. To prevent problems, the blast furnace must be regularly shut off to allow it to cool down or it will melt. If it melts, it would destroy the entire steel mill and kill anyone inside at the time. In this event, the furnace was not shut off and partially melted. Fortunately, no one died. A desperate, quick-thinking engineer with a fire ax hacked apart the main power line into the mill with minutes to spare. While was not specifically a smart building but a smart factory, the cyberattack nearly killed several people and nearly destroyed a billion-dollar asset – the steel mill.

In the article, "Smart Buildings, Dumb Security," the author notes that smart building vulnerabilities are found "at the device and sensor level, at the gateway and controller levels and up to the data, application and network levels."

For improvement he suggests, "As for any security posture, things like strong authentication and access control should be the first step with regard to protection, followed by best-of-breed network, device and application security."

Solving the Security Issues

Both physical and cyber security are important to smart buildings. The Trusted Computing Group's (TCG's) Trusted Platform Module (TPM) and Trusted Network Communications (TNC) specifications provide tools for establishing trust and increasing security in PCs and communication networks. With TPM 2.0, smart buildings and other computing/communications applications can

take advantage of the years spent to develop these standards and the resulting products for enterprise protection.

In a smart building with the TPM and the TCG TNC network security architecture, data across the network and in the cloud is protected and credential authentication ensures authorized physical access to the smart building as well. Figure 1 shows the IoT sensors and actuators of a smart building managed by a cloud-based building management application remote to the sensors. The server and the IoT devices are connected over the public Internet using an OpenSSL connection that supports Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Mutual authentication of devices is required at the session start.

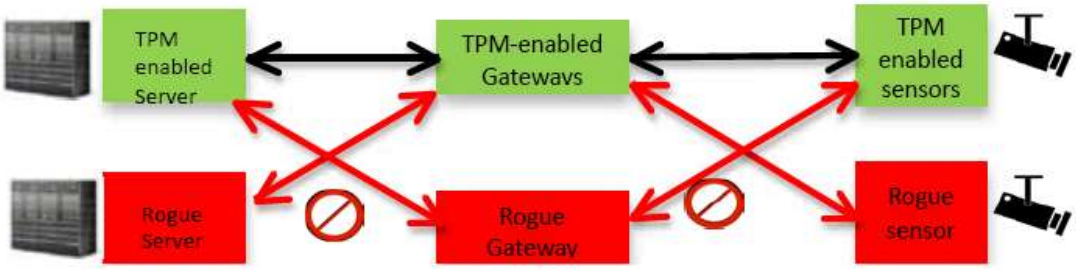

Figure 1. TPM protection implemented in a smart building infrastructure. Enterprise (green) devices use a TPM to protect an enterprise certificate and a device integrity report. Rogue (red) devices lack a valid certificate and/or a recognized integrity report.

In this example, TPMs protect credentials and TNC validates credentials for an enhanced Open SSL authentication process that requires a certificate and an integrity report both protected by a TPM on each device.

TPMs provide proven solutions for unique device identity including Public Key Infrastructure (PKI) and its implementation in protocols such as TLS and enable the use of a range of information security principles. TPMs pair easily with a software-based PKI to build and maintain device identity providing protection for private elements cryptography and enabling interconnectivity assurance.

> "As for any security posture, things like strong authentication and access control should be the first step with regard to protection, followed by best-of-breed network, device and application security." Robert B. Razavi in "Smart Buildings, Dumb Security"

Conclusion

The solution to cyber protection in smart buildings and any IoT application has three aspects:

1. Implement security and identity verification at the earliest stage.
2. Ensure service providers are capable of maintaining security and providing oversight
3. Leverage established standards covering authentication, authorization, encryption, and data integrity

It is important to note that each deployment will have its own needs and require solutions that are flexible and adaptable to address the unique aspects of the application.

References:

[1] "What is a Smart Building?" Building Efficiency Initiative Organization, http://www.buildingefficiencyinitiative.org/articles/what-smart-building

[2] http://www.marketresearchstore.com/news/global-smart-building-market-set-for-rapid-growth-105

[3] Robert B. Razavi, "Smart Buildings, Dumb Security," https://securityintelligence.com/smart-buildings-dumb-security/

[4] "Guide to TCG Seminar and Demonstration Showcase," RSA® Conference 2016, Feb 29- March 4, 2016, Moscone Center, San Francisco

[5] "How to Increase the Security of Smart Buildings?" Communications of the ACM, Vol. 59 No. 5, Pages 47-49, http://cacm.acm.org/magazines/2016/5/201602-how-to-increase-the-security-of-smart-buildings/abstract

[6] GSA & Smart Buildings https://www.gsa.gov/portal/category/100731