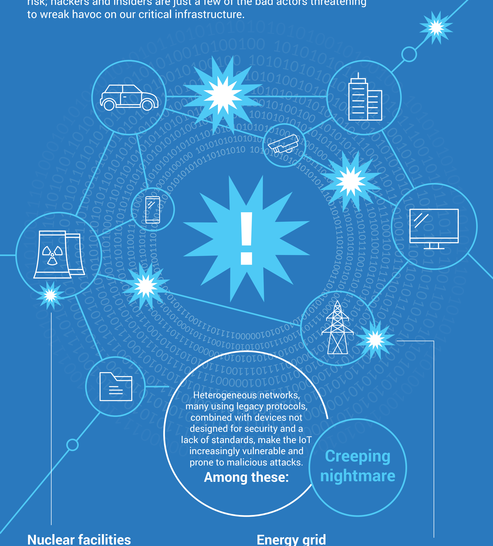
Securing the Internet of Things

Our increasingly connected web of devices is exposed to extreme risk; hackers and insiders are just a few of the bad actors threatening to wreak havoc on our critical infrastructure.



Heterogeneous networks, many using legacy protocols, combined with devices not designed for security and a lack of standards, make the IoT increasingly vulnerable and prone to malicious attacks.

Among these:

Creeping nightmare

Nuclear facilities

The National Nuclear Security Administration experienced 19 successful intrusions into systems that manage the U.S. nuclear weapons stockpile

19

Energy grid

During the same period (between 2010 and 2014), the Department of Energy recorded:

1,131 cyberattacks

159 successful breaches

50B

Along with various utilities and infrastructure, there's a common thread within these systems, called the Internet of Things (IoT). Researchers predict that by the year 2020, the IoT, deployed to control and gather data, will consist of 50 billion connected devices.

1B

TPM

Providing a secure hardware basis for trust, the Trusted Platform Module (TPM) specification has already been implemented in more than one billion devices.

Vehicle Hacking

Cars are highly vulnerable, given their increasing connectivity and digital content. According to the Vehicle Hacking Vulnerability **Survey, among consumers:**

33% have classified car cyber-attacks as a "serious" problem (35% classify them as "moderate")

58% don't believe a permanent solution to vehicle hacking will ever be found

41% plan to keep hacking incidents in mind when shopping for their next vehicle

Data transmission between the factory or third parties and vehicles

Integrity of embedded electronic control units (ECUs) controlling vehicles' operation

TPM 2.0

The TPM 2.0 Profile Specification allows subsets of proven security to be implemented in a variety of devices, from traditional clients to embedded and IoT systems, with smaller footprints, lower power consumption, and lower cost.

Trusted computing, including the TPM and Trusted Network Communications protocols, has been shown to ensure secure software updates in cars. Self-encrypting drives (SED) can protect owner/driver personal data throughout its lifetime.

Smart Buildings

In today's highly automated smart buildings, trusted computing can protect physical security systems, video systems, and cloud-based data transmitted through these systems.

Management applications
- energy management
- submetering
- lighting controls
- remote surveillance & security

Fire & alarm detection
- smoke detection & extraction
- security
- BACS (Building Automation and Control Systems)

Lighting
- building automation
- HVAC controls (heating, ventilation, air-conditioning)

Trusted Computing Group (TCG) Technology

TCG technology (TPMs to protect credentials and TNC to validate credentials) is applied by extending OpenSSL authentication, which requires a certificate and an integrity report, both protected by a TPM on each device; mutual authentication of devices is required at session start.

TPM enabled server

TPM enabled gateways

TPM enabled sensors

Using the TCG specifications and arming devices with TPM can yield significant savings and improve occupant experience in smart buildings, in particular by retrofitting older buildings with sensors and actuators.

Printers and Copiers

The TPM, secure TCG standards-based connections, and TCG standard self-encrypting drives are also securing printers and copiers in offices worldwide.

TCG specifications are ensuring data does not leak to unauthorized users, preventing internal storage intrusion, document theft and network snooping.

As more critical systems are connected to the Internet of Things, strong security is increasingly essential. However, software-based security has proven to be inadequate due to the inevitable presence of software vulnerabilities, which can be easily exploited. The hardware security provided by TPM is a much more effective way to secure the IoT.

www.trustedcomputinggroup.org

SOURCES: Wired, CNet, LinkedIn, USA Today, Coughlin Associates, Trusted Computing Group, Intel, PC World

TRUSTED® COMPUTING GROUP