Trusted Computing Group (TCG)
Embedded Systems Work Group Response
US Federal Trade Commission
FTC Seeks Input on Privacy and Security Implications of the Internet of Things

Executive Summary

The Trusted Computing Group (TCG) is a non-profit organization that creates open standards related to information security. The standards created by TCG are widely implemented across all sectors to address the formidable threats posed by sophisticated attackers. This document describes the technology and standards developed by TCG, documents related to best practices, points out the gaps, and recommends next steps. The complete list of recommendations is summarized at the end of the document.

Introduction into the Trusted Computing Group

Trust and security are fundamental requirements for commercial and private usage of modern information and communication technology. Users, enterprises, and governments are using digital processes through Internet of Things (IoT) every day in mission critical operations like trading, banking, the operation of critical infrastructures, and many others.
The security properties needed to operate safe and dependable computing systems include:

- Secure authentication to provide access to services and data only to authorized persons and organizations
- Secure update mechanism with the following three enhancements: Check current device status remotely, confirm the completion of the software update and enable the creation of certifiable logs for audit purposes
- Data and system integrity to be able to trust into retrieved information and services
- Secure data storage to protect confidential information
- Availability of data and services
- Privacy protection
- Safety and error tolerance

As computing power, availability of information, and access to data and systems have fundamentally changed over the last years, the possibilities to attack systems have also increased. Most computer attacks do not focus on breaking encryption algorithms – which would be difficult with modern ciphers – but against system integrity. Here the properties of the device are manipulated so that keys or other critical data can be retrieved.

The Trusted Computing Group (TCG) has been aiming to define the necessary components to improve trust and security in computing systems. The main goal is to establish trust, which means that you get assurance that the system is always acting in the expected way.

The results of this effort – known as Trusted Computing (TC) – have found their way already into hundreds of millions of PCs, laptops, servers, mobile phones, and hard disk drives. The Trusted Computing Group also defines the necessary infrastructure components that will build the basis to solve the above mentioned challenges. With broad membership including AMD, Cisco, Fujitsu, HP, IBM, Infineon, Intel, Juniper, Lenovo, Microsoft, Wave, and more than 100 other companies, the TCG has direct influence in a huge portion of today's IT market.

The core components of TCGs specifications are the so-called roots-of-trust which are secure hardware components inside the devices. Depending on the specific appliance, these roots-of-trust have different flavors. The first and most popular root-of-trust is the TPM (Trusted Platform Module) which is already part of most newly built PCs.

The TPM is a standardized security product meant to be integrated into a commercial or consumer device. As these devices usually are cost sensitive and have to provide high usability, the TCG specifications have taken these requirements in the design of the TPM.

So how can a TPM make a computer (or a specific consumer device) more secure? In a nutshell, activated TPMs provide the following main functionalities:

- Support system integrity
- Secure authentication and attestation

- Secure storage
- Foundation for trusted operating systems and application software

The TPM as a hardware root-of-trust is superior from a security perspective to software-only approaches. The TPM has integrated measures to provide the basis for a system integrity check by securely collecting information about the boot process during system start-up. This information can be provided to authorize parties to check whether the system is in the expected state. It can also provide strong authentication, enabling a device to authenticate itself to a network with hardware protected information using another set of open specifications defined in the Trusted Network Connect (TNC) Work Group in TCG. The secure storage provides an additional option to store system or user keys (or other secrets).

The TCG is also working with government organizations (NSA and NIST from USA, IPA and NICT from Japan, CESG, BSI and ANSSI from Europe are TCG members) to define the requirements of different security and safety problems; from cybersecurity to privacy protection.

For the specific safety and security requirements of embedded applications like automotive systems, the Embedded Systems workgroup from TCG creates specifications (based on TPM functionality) which can be integrated into embedded systems, like the control system of vehicles, and other critical equipment like industrial control, mobile communications, and critical infrastructure systems.

These security features allow trusted embedded computer platforms to counter a huge variety of attacks. Our design considerations include devices that have to be resistant against logical attacks of viruses, Trojan horses, or direct attacks over the network. They also include countermeasures against repeated password attacks so the passphrases used for the authentication cannot be broken by brute-force-attacks. Additionally, our standards support existing security guidelines (e.g. the Common Criteria Standard) for protecting against certain physical attacks.

The main applications using Trusted Computing today are

- **Secure and trusted boot**
  Systems are only providing full capabilities if the booting process was performed in the expected way.
- **Critical data encryption for storage**
  Even if a protected embedded device (like a car) is stolen, the protected control and authentication is protected by the cryptographic key from the trusted elements and accessible only by the rightful owner.
- **Authentication to network**
  Protecting the authentication information necessary to connect to a network.
- **Integrity protection of software against attacks**
  The software can check its own integrity by using the information stored in the trusted components (e.g. to prevent virus infections like the infamous Stuxnet).

There is a tight connection between software and physical systems in embedded control software. There are frequent interactions between control software and the physical system consisting of the controlled objects, the users, and the operation environments. As each system is developed and operated, communication among various stakeholders inside and outside of systems is very important. For dependability, risk communication is crucial. Trusted Computing support can help make secure the physical systems, the control software, and the communications between them.

About the TCG Embedded Systems Working Group

The Embedded Systems Working Group (EmSys) within the TCG especially develops trust and security specifications for Embedded Computing platforms like automotive, industrial control, smart energy grids, avionics, mobile communication devices, and many others. The working group defines use cases for embedded systems and works on an open architectural framework to deploy Trusted Computing technologies in embedded systems to meet the requirements of use cases. The EmSys Members are working to facilitate the integration of higher reliability and security of automobile control systems, such as remote maintenance system equipped with secure update mechanisms. These secure update mechanisms include accurately understanding the in-vehicle software and hardware situation remotely, confirming completion of intended software updates, and storing certifiable records of the related operations/work. These technologies can also be applied to industrial control equipment, mobile communications, and other various systems.

Its members are also engaged in work and contribution to international research projects about security and trust. They are also contributing in other international standardization work on trust and security in automotive systems (like ETSI in Europe) and are therefore able to reflect the newest developments in security for automotive systems.

Response to US Federal Trade Commission RFI

Q1. What are the significant developments in services and products that make use of this connectivity (including prevalence and predictions)?

The standards developed and published by the TCG have reached a significant market acceptance, implementations and impact across all sectors to address the formidable threats posed by sophisticated attackers. Some of these standards are for example the TPM, the TNC and the Storage specifications, which address the security requirements in many areas of the IT- and network industry. The TCG develops the technology and the standards, documents related best practices, points out gaps, and recommends next steps in the related application scenarios, which are useful also in several domains of the Internet of Things.

Q2. What are the various technologies that enable this connectivity (e.g., RFID, barcodes, wired and wireless connections)?

The TCG has specified and published a variety of specifications, which enable and enhance the security of the connectivity in the Internet of Things. Examples for existing specifications are the TPM and the TNC standard, which are constantly evolved and updated to address the upcoming needs and progress in the modern society. Furthermore new specifications can be expected in the near future from the Embedded Systems Working Group, which focuses on the Internet of Things with devices that range from critical infrastructure to personal household devices. TCG believes the developed Trusted Computing technologies can contribute in a meaningful way to the need for embedded or built-in security in the devices that constitute the Internet of Things.

Q3. What types of companies make up the smart ecosystem?

There is a wide support by the members of the Trusted Computing Group, which develop, contribute and promote the technologies and specifications in the ecosystems. The TCG has more than 100 members from across computing, including component vendors, software developers, systems vendors, network and infrastructure companies and others. The TCG offers different levels of membership and the high number of members on the upper promoter and contributor membership levels shows the interest of the companies in these technologies. The current list of member companies can be found online at: http://www.trustedcomputinggroup.org/about_tcg/tcg_members.

Q4. What are the current and future uses of smart technology?

The systems involving Trusted Computing technologies can benefit from the security enhancements in different ways. Trusted Computing enables the

- protection of critical data and systems against a variety of attacks,
- secure authentication and strong protection of unlimited certificates, keys, and passwords that otherwise are accessible,
- establishment of strong machine identity and integrity,
- addressing of requirements of regulatory compliance with hardware-based security.

The Trusted Computing specifications are constantly evolved and extended to consider the current and future uses of the technology in several market segments.

Q5. How can consumers benefit from the technology?

For the consumer the Trusted Computing technologies offer several benefits:

- Provide more secure remote access through a combination of machine and user authentication
- Protect against data leakage by confirmation of platform integrity prior to decryption
- Provide hardware-based protection for encryption and authentication keys used by stored data files and communications (email, network access, etc)
- Protect in hardware Personally Identifiable Information, such as user IDs and passwords
- Protect passwords and credentials stored on drives
- Protect the update mechanisms of software in the Internet of Things.

Q6. What are the unique privacy and security concerns associated with smart technology and its data? For example, how can companies implement security patching for smart devices?

The TCG has set for itself the ambitious goals of improving the security of the platform and infrastructure while:

- preserving privacy, backward compatibility, and owner control
- promoting ease-of-use
- designing the technology so that it is interoperable
- ensuring that the user's data, while secure and protected, remains portable and accessible as needed in alternative modalities

These principles can be also applied in secure update mechanisms for consumer devices in the Internet of Things. Such an update mechanism can be established with the following three enhancements: Check current device status remotely, confirm the completion of the software update and enable the creation of certifiable logs for audit purposes.

Q7. What steps can be taken to prevent smart devices from becoming targets of or vectors for malware or adware?

The Trusted Computing concepts consider platform integrity and malware prevention as central topics for the protection of modern communication devices:

- Platform Integrity: Measures and reports on integrity of platform, including the BIOS, disk Master Boot Record, boot sector, operating system and application software, to ensure no unauthorized changes have occurred.
- Malware Prevention: Relevant functionalities assist to prevent rootkits and other malware by ensuring platform integrity prior to boot. Furthermore it helps administrators to ensure that systems are healthy prior to network connection.

Trusted Computing supports the concepts for a Root of Trust, which allows the computation of inherently reliable integrity measurements. These concepts can also be used to implement secure update mechanisms to protect against malware or adware. This can be also combined with self-healing concepts to consider heterogeneous or autonomous environments like peer-to-peer structures.

Q8. How should privacy risks be weighed against potential societal benefits, such as the ability to generate better data to improve health-care decision making or to promote energy efficiency? Can and should de-identified data from smart devices be used for these purposes, and if so, under what circumstances?

TCG-enabled components are designed and implemented to address the security requirements while supporting the privacy concerns of the users. The TCG specifications support privacy aspects in a variety of ways including the use of zero-knowledge protocols (DAA – Direct Anonymous Attestation protocol) or through a Privacy Certification Authority (CA). The usage of such tools protects the user’s privacy and hinders the data aggregation and the traceability of the end user. These concepts are generic and can be therefore used in many application scenarios like health-care or in the smart grid domain.