International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 2 No. 4 Apr. 2013, pp. 540-546

http://www.issr-journals.org/ijias/

Towards a Trust Envisioned Cyber Security

Renu Mary Daniel and Angela Francis

Department of Computer Science and Engineering,
Karunya University,
Coimbatore, Tamil Nadu, India

ABSTRACT: Ensuring trust in cyber space has become an important and indispensable security challenge. Questions about trust in the physical space can be answered based on the factors namely closeness, time, analyzing actions and body language. But in the cyber space these factors are not readily available correctly to ensure and verify trust. Trust can also be established via a third party. But can we know with absolute certainty that the entity with whom we are communicating is trustworthy or not? Cyber security is all about ensuring that software will behave in an expected manner and that it can prevent any threats that deter it from its expected operations. It not just deals with securing networks but rather focuses on ensuring the security of the devices connected to the networks. In this paper, we discuss the approaches used earlier for establishing trust, their limitations and focus on the need for hardware-based root of trust as software-only solutions are inadequate to ensure complete trust. We discuss an emerging technology in the field of trusted computing called the Trusted Platform Module that provides a hardware-based root of trust. We also discuss about its scope, various applications, and the future work being done on it.

KEYWORDS: Trust, Cyber Security, Trusted Platform Module, Integrity Measurement, Remote Attestation.

1 INTRODUCTION

The basis of security is trust. Trust is defined [Grandison and Sloman, 2000] as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". These notions of trust and trustworthiness are as old as civilization allowing people to act under uncertainty to trust larger corporations, more diverse institutions and more complicated systems. Trust in computing platforms is a topic that spurred widespread research among the scientific community that ultimately led to the concept of trusted computing. So why do we need it?

Our day-to-day life is closely associated with an intricately woven set of communications and transactions that take place in the cyberspace. We depend on these networked information systems for routine and critical tasks and they in turn control all the critical infrastructures. This dependency if not maintained in a trustworthy environment might lead to economic disruption and disaster [1]. Cyber-crime has been an ever present threat to the endpoint, network, data, and other computing devices, [2] but what is actually being done about it? Since its advent, there have been innumerable attempts to ensure trust in the cyberspace, ranging from authentication protocols, digital signatures and third party certificates. None of these could address the security threats in the information space. People and their devices are constantly being invaded by attacks such as malware exploits, zero-day viruses, etc as too much of the personal information is put online.

It is necessary to establish trust in every component of a computing device including the hardware, firmware and software so that we can provide an effective countermeasure against the aggravated rate of security threats. In the physical space trust is established through the identity and behavior of an individual. But in cyberspace the identity of a device can be fabricated and the behavior of the system can be deceptive, there is no means to physically verify the genuineness of the device or its components. With these security aspects in mind, the Trusted Computing Group (TCG) [3], [4] has developed a secure crypto processor chip called the Trusted Platform Module (TPM) for providing a hardware-based root of trust in computing devices.

Corresponding Author: Renu Mary Daniel (renudnl@gmail.com)

The remainder of the paper is as follows: Section 2 details on the current cyber security threats; Section 3 lists the existing security countermeasures; Section 4 analyzes the need for a hardware-based security solution called the TPM; a detailed overview of the TPM and its functionalities is provided in Section 5; Section 6 describes the threats addressed by TPM; Section 7 presents the various applications in which TPM can be deployed; we discuss the scope and future of TPM in Section 8; we conclude the paper in Section 9.

2 THREAT MODEL

The protection of information assets is a concern for computer security. Major aspects for ensuring trust are integrity, confidentiality and availability [5]. Protection through software alone of a PC or other computing platform has developed substantially but with innate weaknesses. The security of the computing systems including laptops, smartphones and other devices, are being threatened by new attack vectors [2]. As these computing devices become more portable and handy, they are more likely to be stolen. Once in the hands of the adversary, they are exposed to a variety of hardware as well as software attacks. Software- only security solutions can be affected by other soft- ware running alongside them on the same platform [10]. Security threats like buffer overflows, code injection and SQL injection [6] are used maliciously to introduce malware into the system and for privilege escalation. In the present scenario a malicious code can obtain access to the sensitive data in the memory by gaining control over the operating system. There should be strong hardware enforced memory isolation to prevent unauthorized memory access to thwart such attacks.

From the advent of e-commerce, hackers have been writing well designed malware to attack the websites and their customers. The communication channel through which these computing devices access the corporate network or the Internet can be attacked in a number of ways posing a threat to the individual's as well as the network's sensitive data. Identity thefts [6], pirated software hosting, spamming, spoofing and phishing [7] are few of the problems faced by online ecosystems. Spoofed emails lure users into executing malicious attachments, which in turn exploits vulnerabilities in the system thereby providing a backdoor to a possible attacker. Once a system gets infected, key-loggers, screen scrappers and sniffers record activities of the user and leak the users secrets to the adversary controlling them. These attacks emphasize the need for secure I/O features in the system.

Data theft or sensitive information leakage is also sometimes related to insiders in an organization. Insiders familiar with the organization's policies, procedures and technology can exploit them to trade with external attackers. The success of such attacks is due to the fact that computing devices fail to provide secure storage for sensitive information like passwords. Today due to intensive computing and networking, if one system in the network is compromised, the entire network can be affected. Attackers are interested in servers and networks because of the sheer volume of data they contain and process. Such attacks are possible because compromised systems can gain access to the network and infect other systems in the network.

3 STATE - OF - THE - ART SOLUTIONS

An ultimate solution is not possible for the security of computing devices. However, an account of the solutions relevant to the security threats discussed above is presented here. To keep track of vulnerabilities and infections, the operating system and applications should be regularly updated and patches should be installed so that they are not exploited by e-mail viruses, internet worms, backdoor trojans, etc. To prevent unauthorized memory access, sandboxing is a mechanism that separates running programs. It is a specific example of virtualization as it is used to run untrusted code with a tightly controlled set of resources. Data loss prevention software or content monitoring is used to prevent the loss of data and for content filtering. End-to-end reliable secure services provided by SSL [5] can be used to secure user information during online transactions. Before granting access to a website a two-factor authentication can be deployed to validate user's identity. But even authentication exchange and digital signatures will fail if the system is infected by a rootkit or a bot [7], as the software running on it will be corrupted. Another strong technology used to secure computing systems is the use of biometrics. A high level of security is offered by finger-print authentication by providing access to data by simply swiping a registered finger. The insider attack can be controlled by incorporating the "least privilege" approach which allows employees to access just the information that they need.

4 NECESSITY FOR A TRUSTED COMPUTING MODULE

As discussed above there are various existing security technologies such as firewalls, security softwares such as antivirus software, cryptographic accelerators and security protocols such as Secure Socket Layer (SSL) etc. to mitigate the plethora of threats associated with the computing devices. Most of the security software runs on the main processor with the

assumption that its running in a safe environment. Secrets that are stored as normal data or in protected files or hard disk partitions are vulnerable and can be exposed to malicious programs. Encrypted data whose encryption keys are stored in the hard disk can be attacked as the hard disk can be tampered. Security softwares can also be attacked by viruses and thus do not provide reliable protection. Cryptographic accelerators are composed of specialized hardware and firmware that provide a protected environment for secrets and can do bulk encryption in physically protected environment. However they are too expensive and do not have a Core Root of Trust for Measurement (CRTM) [11] built into the boot process. A trusted hardware creates a foundation of trust for software processes. Thumb-sized chips called smartcards are secure platforms available at a low cost, due to which they have become widespread. Although multiple applications from different vendors are allowed to exist side-by-side, due to the limited resources available, complex applications are not supported. The Trusted Platform Module (TPM) [13], [14], now included in almost 500 million laptops, is a built-in hardware chip which builds a stronger trust and confidence in computing platforms. The TPM revolutionized the digital security industry by providing a hardware-based solution. TPM provides the mechanism to generate keys based on a combination of the identity of the software trying to access them and the identity of the system. It releases the keys only if the system is in an unmodified trusted state.

5 TRUSTED PLATFORM MODULE

The TPM 1.2 implementations are stand-alone chips which are soldered on the motherboard of a computer on the LPC bus or integrated into a custom PCB for an embedded device, they communicate with the rest of the system by using a hardware bus. A TPM should support the following core functionalities: secure storage, platform integrity reporting and platform authentication [10].

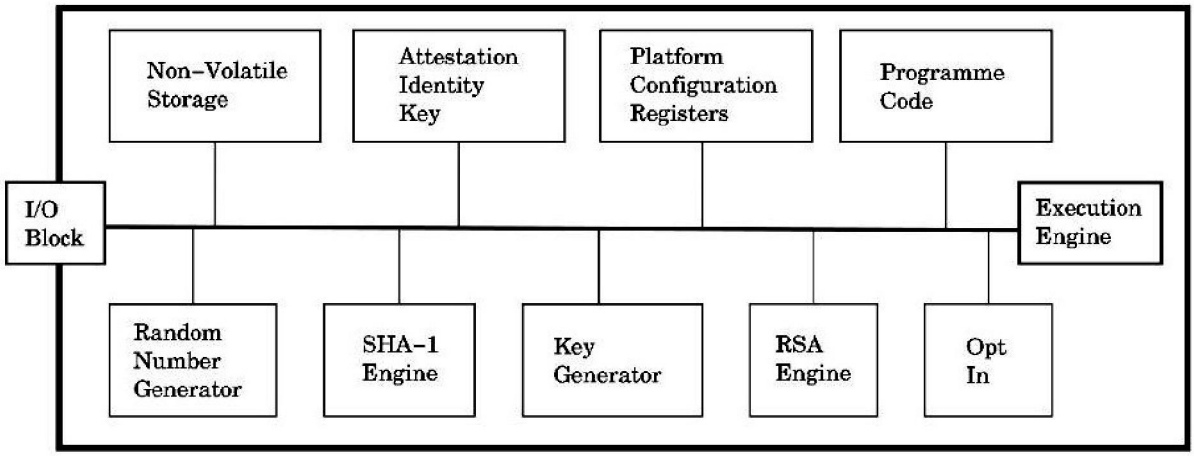

Fig. 1. TPM Architecture

Fig. 1 shows a detailed architecture diagram of the Trusted Platform Module.

5.1 TPM COMPONENTS

TPM is the hardware realization of the TCG specifications. It enhances the level of trust in networks and computing devices. TPM is a passive (slave device, that does not control or prohibit the normal execution flow of the system and does not have access to the system resources), opt-in device, which provides privacy-enabling functions when activated. According to the TCG specification [4] it is not mandatory for a TPM to be implemented as an IC. Developers are to implement this functionality, either in hardware or software.

The I/O block allows data to be transported over virtually any bus or interconnect, it manages information flow between the components and between the TPM and external bus. The flags maintained by the Opt-In block determine the access rights. The non-volatile memory in the TPM stores two long-term keys i.e. the Endorsement Key (EK) and the Storage Root Key (SRK) which forms the basis of key hierarchy. It is also used to store the owners authorization data (owner's password). The Endorsement Key (EK) which is unique to the TPM, is embedded in it. More precisely, a TPM has an endorsement key pair, whose private key never leaves it. The EK pair is provided by TPM manufacturers and stored in the tamper resistant non-volatile memory before shipping the TPM [11].

The private EK is never used to generate signatures. The process of encrypting data sent to the TPM during the process of taking ownership and the process of creating AIK certificates uses the public EK. The Attestation Identity Key (AIK) regarded as an alias for the Endorsement Key may also be stored within the TPM. Multiple AIKs are supported by a TPM, this helps to maintain anonymity between different service providers who require proof of identity. To make the AIKs persistent, they should be stored in secure external storage. A volatile storage area in the TPM is provided where one or more AIKs can be loaded when in use. The Platform Configuration Registers (PCR) are used to store integrity metrics which measure the integrity of any code, from BIOS to applications, mainly before the execution of the code.

These registers are reset on power-offs and restarts. They store 160-bit values which are SHA-1 digests. In TPM v1.1 there are 16 PCRs (0-15), but in the latest TPM v1.2 there are 24 or more PCRs, in v1.1 specification the PCR values will be reset only when the sys- tem is rebooted, registers 0-7 are reserved for TPM use and register 8-15 for operating system and application use. While in v1.2 specification there are static and dynamic PCRs. Specifically, PCR 0-16 (static PCRs) will be reset to 0 by a system reboot, thus providing a static root of trust for measurement (SRTM) and PCRs 17-22 (dynamic PCRs) can be reset to 0 without a system reboot or to 1 with a system reboot, providing dynamic root of trust for measurement (DRTM). The Programme Code is the root of trust for integrity measurements which is referred as the Core Root of Trust for Measurement (CRTM) [13]. The Execution Engine runs the programme code described above.

TPM chip contains a Random Number Generator (RNG) that can seed random numbers to induce randomness in key generation, nonce creation and to strengthen passphrases. SHA-1 Engine is used to generate AIK blobs, computing signatures and for other general purpose use. RSA Key Gneration and RSA Engine is used to produce 2048-bit modulus storage and signing keys (SRK and AIKs) using the RSA algorithm. TPM chips will be in ready-to-be-owned state when the devices are shipped [14]. Depending on the user discretion, its state can vary from disabled and deactivated to fully enabled. Opt-in facility maintains the physical state of the TPM and applies the disabling feature to all the TPM components as per the user directions.

5.2 TPM FUNCTIONS

5.2.1 SECURE STORAGE

A TPM can store secrets securely. As the TPM has limited storage space, it allows to store keys, and other data needs to be protected. This limited storage can be extended by exporting keys in encrypted form (encrypted using SRK or some other storage key), that are decrypted only when loaded back into the TPM. The private key of the SRK never leaves the TPM. Binding and sealing are the two mechanisms provided by TPM for secure storage [4], [13], [14]. Binding refers to the encryption of data using a key managed by a particular TPM. The bound data inside the TPM can be decrypted using the private key (unbinding). Sealing refers to encrypting externally provided data with reference to a specific PCR state along with a nonce specific to a particular TPM using a storage key. It is a way to combine the measurements (PCR content) and external data. Unsealing refers to loading the key used for sealing into the TPM and decrypting the blob, if the nonce does not match the one of the TPM or if the specified PCR values do not match the platforms current PCR values, it returns error.

5.2.2 INTEGRITY MEASUREMENT

The process of obtaining configuration parameters of a platform is known as integrity measurement [9]. The goal of integrity measurement is to measure system state into the PCRs [4].

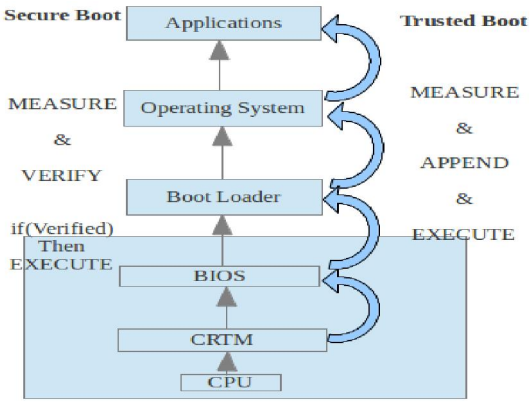

Fig. 2. Secure Boot vs. Trusted Boot

The steps involved in this process are to measure (compute the hash value of) the next entity, e.g. BIOS measures the integrity of the OS Loader, the OS Loader measures the integrity of the operating system and this process continues up to the user level applications. The measurement is made by creating a SHA-1 digest of the code to be loaded (SHA-1(data)) and extended (appends the new measurement to the old PCR value) into one of the PCRs. Measurements change with system updates and patches.

5.2.3 REMOTE ATTESTATION

Attestation provides a current platform state stored in the Integrity Measurement Architecture (IMA) to the remote entity for platform authentication [13], [14]. IMA contain the log of software events stored as mea- surements and extended to TPM's PCRs. Attestation involves a challenge-response protocol [12]. A remote verifier (challenger) sends a challenge consisting of a nonce (to thwart replay attacks), and a list of PCR in- dices. The response consists of the current PCR values of the listed PCR indices, along with a quote. Quote is a digital signature computed within the TPM, over the aggregate of the list of PCR values and nonce received from the challenger, using private AIK.

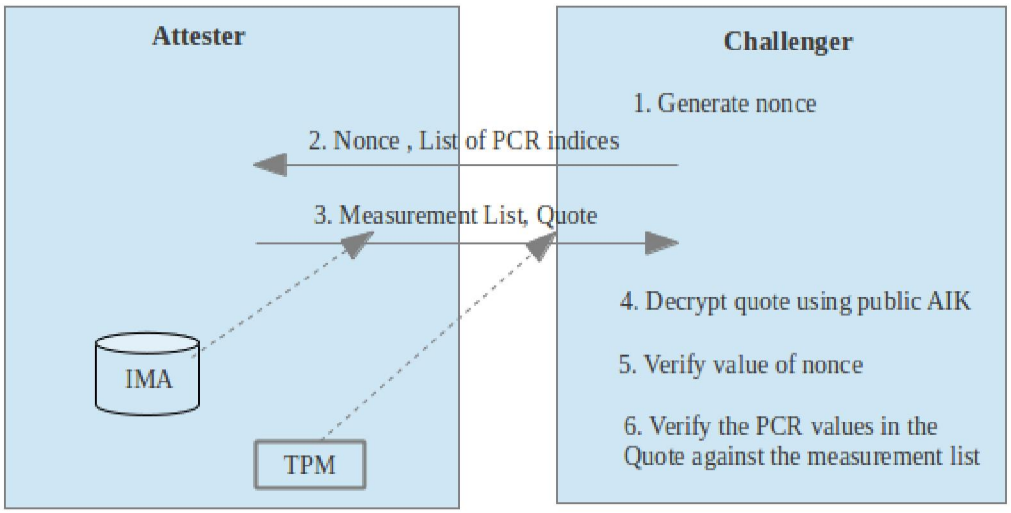

Fig. 3. Remote Attestation

The challenger upon reception of the response should verify the following:

- The value of nonce in the reply.
- Decrypt the quote using the public AIK obtained through authenticated channel.
- Verify whether the list of PCR values matches those included in the quote.
- Verify whether the PCR values itself represent an acceptable and secure boot sequence.

6 THREATS ADDRESSED BY TPM

Threats associated with the Web such as virus attacks, identity theft, unauthorized access [8] to the platform can be mitigated by the mechanisms provided by the TPM. TPM enables users to vouch for the integrity of the platform. The integrity measurement and reliability of a platform is done by the TPM by taking a SHA-1 digest of the code and extending it with the existing PCR values. A customer can verify that a service provided by a service provider is trusted by a function provided by TPM called attestation. It allows the communicating entities to remotely exchange and verify their platform integrity before initiating the communication to ensure trust. This technique helps prevent online fraud. TPM also protects the sensitive data from hacker scripts by sealing them with cryptographic keys to a particular platform state, known only by the owner. Even though the script executes, secrets cannot be accessed. It resolves data theft by providing a secure, tamper-proof environment called Root-of-Trust for Storage, for computing and storing the keys. This protected capability will release the keys for computation, only to functions that have exclusive permission to access shielded locations in the chip. An adversary can find a secret in encrypted form, but will not be able to view it in clear. In other words, TPM ensures that secrets belonging to different people are not revealed to others. Users, business partners, service providers and customers can communicate with each other only exposing the data they intend to be exposed. A TPM helps in maintaining the confidentiality of an organization's information by providing secure digital signatures.

7 APPLICATIONS

There are a number of reasons why TPM chips are useful. For example, they permit online service providers to verify the platform authenticity through secure booting and integrity measurement, thereby reducing online fraud and identity theft [2]. A website could also be verified by a consumer if its a legitimate merchant site or not using TPM technology. Hardware-based security provided by the TPM can be used to encrypt emails, and for improving protection for VPN, wireless networks, file encryption and password/PIN/credentials' management. User authentication can be provided by augmenting the device with TPM features likes sealed storage along with normal security practices like finger-print biometrics, smart cards [11] and passphrases. Already a transition is well underway to use TPM-based security in mobile devices which access the restricted information in government and other networks. Attempts to incorporate TPMs in VANETs [15], cloud computing networks, grids are in progress and soon it will be included in security sensitive devices like electronic voting machines [16] and biomedical equipments.

8 SCOPE AND FUTURE WORK

As mobile-phone embedded computers are gaining popularity, with the host of interesting services that they provide including Javascript and interactive web-services, TPM can be deployed for controlling and monitoring these devices. TPM can even be incorporated in tape drives and USB drives. Full disk encryption applications like TrueCrypt, BitLocker drive encryption can make use of TPM to protect the keys, encrypt hard disk and provide trusted boot through integrity measurement. TPM can be added to network devices for authentication of requests, before allowing access to resources. A future home network with Internet-capable devices can be safeguarded using a TPM this will prevent the stealing of the Home Key [17]. The TPM also plays a vital role in the Windows 8 operating system by providing remote attestation by trusted third parties. It provides a trusted boot mechanism called the hardened UEFI BIOS standard. There is a future for TPM in protecting credentials for authentication, where TPM stores credentials of users for different services. Each user will just have to remember a unique access code for a TPM-enabled device, which can then provide the access credentials for all the required services in complete isolation with other user accounts. As TPM cannot mitigate some hardware attacks, plans are underway to release specialized hardware with more tightly integrated TPMs, as the TPM specification does not require it to be a separate chip.

9 CONCLUSION

Cyberspace has entered the realm of reality, it is no longer a science fiction. Our increased dependency in this virtual world of networked information systems emphasizes the need to ensure trust in these devices. Any kind of disruption in their operation can put life, property and economy at stake. In this paper, we have surveyed the security threats in the cyberspace and have elaborated on the countermeasures to those threats. Having mentioned the countermeasures, we identified that these countermeasures were inadequate to ensure complete trust of an end system. As the underlying security mainly depends on the hardware, the TCG's TPM is capable of providing a hardware-based root of trust, which increases the overall security of the computing devices. Further we have provided a detailed account on the necessity of a trusted computing module and the various application areas it can be applied to. With various innovations taking place in the area of trusted computing TPM still has a long way to go.

REFERENCES

[1] Virgil D. Gligor, and Jeannette M. Wing, "Towards a Theory of Trust in Networks of Humans and Computers," *Carnegie Mellon University Research Showcase,* 2011.

[2] Nor Fatimah Bt Awang, "Trusted Computing-Opportunities & Risks," *Collaborative Computing: Networking, Applications and Worksharing, IEEE*, 2009.

[3] Trusted Computing Group, Incorporated, "TCG specification architecture overview," 2007.

[4] A. Sadeghi, M. Selhorst, C. Stuble, C. Wachsmann, and M. Winandy, "TCG inside?: A note on TPM specification compliance," *Proceedings of the first ACM workshop on Scalable trusted computing, ACM*, pp. 4756, 2006.

[5] Hatoon Matbouli, and Qigang Gao, "An Overview on Web Security Threats and Impact to E-Commerce Success," *International Conference on Information Technology and e-Services, IEEE*, 2012.

[6] A. Esma, and S. David, "The ultimate invasion of privacy: Identity theft," *Ninth Annual International Conference on Privacy, Security and Trust, IEEE*, 2011.

[7] M. Tariq Banday, Jameel A. Quadri, and Nisar A. Shah, "Study of Botnets and Their Threats to Internet Security," *Sprouts: Working Papers on Information Systems*, 2009.

[8] Norman Schneidewind, "Metrics for Mitigating Cybersecurity Threats to Networks," *Internet computing, IEEE*, pp. 6471, 2010.
[9] Junkai Gu, and Weiyong Ji, "A secure bootstrap based on trusted computing," *International Conference on New Trends in Information and Service Science, IEEE,* 2009.
[10] Bryan Parno, Jonathan M. McCune, and Adrian Perrig, Bootstrapping Trust in Modern Computers, ISBN 978-1-4614-1459-9, *Springer*, 2011.
[11] Keith E. Mayes, and Konstantinos Markantonakis, Smart Cards, Tokens, Security and Applications, ISBN-13: 978-0-387-72197-2, *Springer Science+Business Media, LLC*, 2008.
[12] Dries Schellekens, Brecht Wyseur, and Bart Preneel, "Remote Attestation on Legacy Operating Systems with Trusted Platform Module," *Electronic Notes in Theoretical Computer Science 197, Elsevier,* 2008.
[13] Sundeep Bajikar, "Trusted Platform Module (TPM) based Security on Notebook PCs White Paper," *Intel Corporation*, 2002.
[14] Siani Pearson, "Trusted Computing Platforms, the Next Security Solution," *HP Laboratories, Hewlett-Packard Company,* 2002.
[15] Asif Ali Wagan, Bilal Munir Mughal, and Halabi Hasbullah, "VANET Security Framework for Trusted Grouping using TPM Hardware," *Second International Conference on Communication Software and Networks, IEEE,* 2010.
[16] Russell A. Fink, Alan T. Sherman, and Richard Carback, "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *IEEE Transactions on Information Forensics and Security, IEEE,* 2009.
[17] Holger Kinkelin, Ralph Holz, Heiko Niedermayer, Simon Mittelberger, and Georg Carle, "On Using TPM for Secure Identities in Future Home Networks," *Future Internet,* 2011.