International Journal of Social Sciences and Management Review

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

HARDWARE ROOT OF TRUST BASED TPM: THE INHERENT OF 5IRECHAIN SECURITY

VILMA MATTILA, PRATEEK DWIVEDI, PRATIK GAURI & DHANRAJ DADHICH

5ire (Sustainable Distributed Computing)
Unit Number 101, IFZA Dubai - Building A2, Dubai Silicon Oasis,
United Arab Emirates

https://doi.org/10.37602/IJSSMR.2022.5319

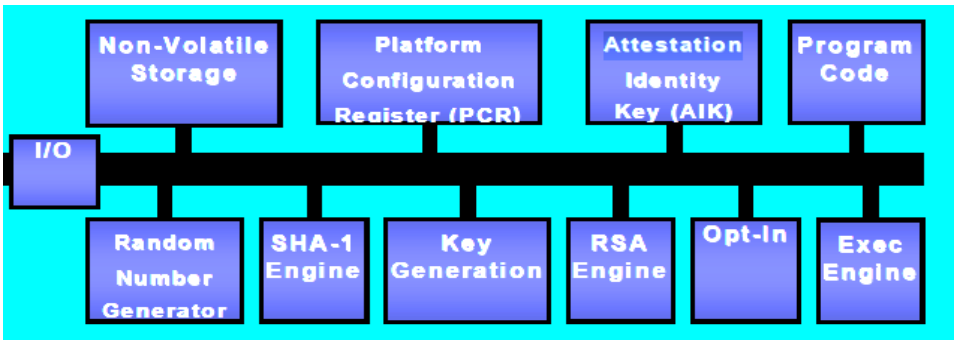
ABSTRACT

The hardware root of trust is already a critical component of the security architecture of enterprise and government networks that allows for efficiently deployed and managed data protection across the entire data life cycle. For all these reasons, the TPM will be a major area of attention for security professionals today and tomorrow. The 5ire ecosystem ensures that all the nodes in the blockchain ecosystem establish a certain level of trust. A hardware root of trust based on the Trusted Platform Module (TPM) is introduced for this purpose. A TPM device will allow the 5ire nodes to remotely attest the devices for any malicious code.

Keywords: TPM; Trusted Platform; 5irechain Security; Privacy

1.0 INTRODUCTION

In the IT and security worlds, a lot has changed in these years from maturity and a threat perspective that is driving increased adoption of TPM. Nowadays, a number of key factors are driving intense interest in TPM among enterprise security professionals and IT managers. Meanwhile, threats that take advantage of software-based protections are driving security lower in the stack. The Trusted Platform Module (TPM) is a hardware module that is currently deployed in many commercial desktop and laptop PCs, servers, etc. The objective of a TPM is to provide a hardware-based root of trust for a computing system. The figure below shows a generic architecture for the TPM taken which provides various basic functions including (a) cryptographic functions such as random number generation, key generation, and encryption/decryption, (b) SHA-1-based integrity measurement, (c) internal storage for protecting keys and logged measurements, (d) sealing and binding operations.



Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

Figure 1: Generic architecture of a Trusted Platform Module (TPM)

2.0 FUNCTIONALITIES OF THE TRUSTED PLATFORM MODULE (TPM)

The TPM has various functionalities from which a distinction can be made. These are platform authentication, secure storage, platform measurement, and reporting.

At the time of development, a special unique public/private key pair, called the Endorsement Key (EK) was set. Additionally, when taking ownership of a TPM, another special key is generated called the Storage Root Key (SRT). The EK and SRT are long-term keys and since these are identifiable are not meant for the signing but only for encrypting. In order to do a signing of application-specific data with the TPM, Application Identity Keys (AIK) can be generated. AIK's opposed to SRT and EK can be proven to be generated by a TPM but not which TPM to ensure user privacy. This is done through the use of privacy certification authority (privacy CA) where EK can be used to prove an AIK is from a TPM without revealing which TPM. Addition, another way is by using Direct Anonymous Attestation (DAA) which is based on group signatures. DAA has the advantage over privacy CA by allowing the key creator to choose whether EK and AIK have any association or their relation is completely anonymous

One can store data securely by using keys generated by the TPM. The TPM consists of a Hashing engine, RSA key generation, RSA signing and encryption, and also a Random number generator which can be used in the generation of keys.

Platform Configuration Registers (PCR) play a vital role. These are registers in the TPM that can compute hashes or also known as measurements of a component and store it. These measurements can be extended which means that the current PCR value is the accumulation of all the measurements it has stored. The PCR value can be used as an authentication signal by for example assuring the state of a platform to a third party or ensuring data is only accessible to authorized software.

However even though TPM capabilities have penetrated the markets for PCs, servers, and other non-traditional devices, TPM has to date not been adopted on a large scale by enterprises due to the delay is related to a mix of issues with manufacturers, the nature of upgrade cycles, compatibility with other security software and protect devices at a lower level. Now, however, an increasingly complex threat landscape, coupled with the widespread availability and increased maturity of the TPM technology as well as other factors such as cost reduction makes TPM ready for prime time. The TPM 2.0 specification was recently published for additional protections such as protected storage and shielded execution.

At the current moment, a modern version called TPM 2.0 is already in use. TPM 2.0 shares the same functionalities as its predecessor TPM 1.2 except with some additional functionality and improvements as listed below in the table below:

Functionality	TPM 1.2	TPM 2.0
Algorithm agility	Sha-1 hash algorithm	Virtually any hashing algorithm

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

Authorization	Needs owner authorization	Uses clever policy decision to decide authorization
Key Loading	time-consuming private-key decryption	quick symmetric-key operation
Fragility PCRs	Brittle PCR because sealing to PCR value approved by particular PCR value	Non-Brittle PCR because of sealing to PCR value approved by a particular signer
Management	Difficult to give authorization for different roles	Built-in different authorizations, policies and hierarchies
Identifying Resources	By handle where the user could be tricked into authorizing a different action	By name of which the resource is cryptographically bound to

3.0 TRUSTED PLATFORM MODULE (TPM) IN 5IRECHAIN

- Security to Scale: TPM allows 5irechain to protect secrets and data that are worth money to cybercriminals. Software-based security is regularly defeated. Hardware encryption mechanisms like TPM are well suited for 5irechain with the scale and complexity of systems and systems management. This is one of the reasons the National Security Agency (NSA) and NIST both recommend the concept of hardware-based security. The National Institute for Standards and Technology (NIST) acknowledges the risk with software and software-based security in SP 800-164, "Guidelines on Hardware-Rooted Security in Mobile Devices. According to the NIST documentation, the currently available way to do this is to:

- Measure firmware, software, and configuration data before it's executed

- Store those measurements in a hardware root of trust, like a TPM

- Validate that the measurements made actually match the measurements that were expected

- Supports Audit: The TPM enhances 5irechain security and the security audit process with confidence which is a critical concern for many organizations today. Because the system can attest to the state of the device and whether or not it blocked access based on that attestation, this data can be drawn from the platform management system for use in audit and investigations.

- Beating Bootkits and Other Malware: While no security is 100 percent tamperproof, the security processes of 5irechain enabled by TPM present far stronger protections of endpoints and their data than anything currently offered by software security.

- Enhanced Encryption: With the growing use of mobile devices to process company information, along with collaborative applications shared between devices, encryption is more important than ever. However, ease of use is a critical factor in encryption for today's on-the-go user population. TPM also greatly enhances the software-based encryption key management mechanisms of Windows BitLocker, which otherwise requires that encryption keys be offloaded to a USB drive, introducing significant cost and management issues. TPM supports the software-based encryption mechanisms used to encrypt the contents of desktop and notebook hard drives, including Microsoft's BitLocker drive encryption, which is

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

included in most of the current corporate versions of Microsoft Windows. BitLocker is a form of software-based full-disk encryption that relies on a TPM to verify the integrity of the platform at boot. BitLocker on Windows 7 uses the TPM to validate boot integrity and to secure encryption keys. For Windows 8, boot-level protection is now handled through Microsoft's Unified Extensible Firmware Interface (UEFI) instead, although TPM is used for securing encryption keys. Through these changes, Microsoft has significantly enhanced the BitLocker back-end management product, MBAM, for central deployment and administration of BitLocker keys, including unlocking encrypted computers—for example, when users have forgotten their PINs or passwords.

- Support for Virtualization: Upgrade cycles and especially hardware upgrade cycles can take years, but factors like virtualization and cloud computing, consumerization and bring your own device (BYOD) policies are rapidly shortening the typical upgrade cycle.

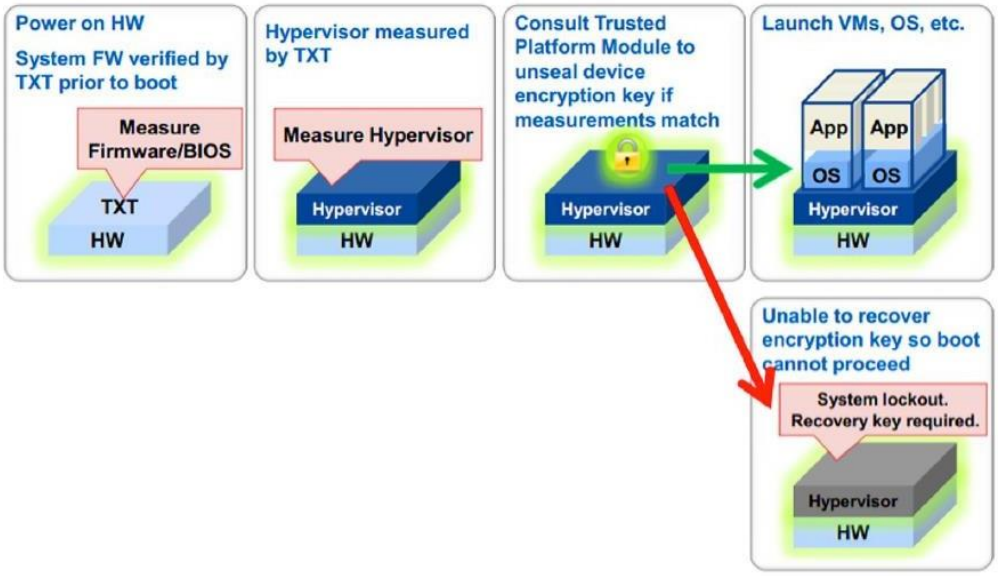


Figure 2: TPM in Virtual Environment

5irechain uses a feature of the TPM specification called "sealing" to ensure that secret data is decrypted and used only when there is no doubt the platform has not been compromised. When the system boots up, integrity measurements are taken and stored in Platform Configuration Registers (PCRs) in the TPM. It's possible to order the TPM to encrypt data and tie decryption to a conditional state of the device, so it is decrypted only if the values stored in the PCR match specified values and the platform is in a verified clean state.

- Remote attestation: A TPM in 5irechain can be used to provide this method which allows for an entity to authenticate itself, in terms of software, hardware, or both, with another, remote, entity. In a way, the entity proves to the requester that it is trustworthy and that its systems have not been tampered with. The basic functioning of this operation is similar to how integrity measurement works, as it serves as the basis of the attestation process, with it then being transmitted to the requester. The process works as follows: the requesting entity sends a request to the remote entity, where a nonce is included. The receiving platform will then forward the request to the TPM that will perform an integrity measurement, and also sign the nonce sent to it. This is then sent to the requester that will verify the response with a

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

trust attestation authority (TAA), verifying that (a) the TPM is genuine and (b) that the received values match the known values. If everything is correctly verified, the requester will consider the entity to be trustworthy.

- Integrity measurement: The TPM can be used for verifying data integrity of 5irechain. There are two main perspectives on types of integrity measurement: static, where the measurement is made on binaries or firmware, before they are run, to ensure that no tampering has happened, and dynamic, where changes are monitored and detected during run time, to ensure that no tampering or unauthorized changes were done.

- Generation and secure storage of keys: Cryptographic keys can be both generated and stored in the TPM, to be then securely used by, that is, a VM. The TPM can generate random secure keys, using entropy both within and outside of the TPM. Keys can then be generated through three different methods: from seed, from a random number generator, or directly imported to the TPM. The keys are then securely stored inside of the TPM. External keys can also be stored inside of the TPM, where they are encrypted with the public part of the storage root key (SRK), a key pair generated inside of the TPM.

- Trusted boot: The TPM can use integrity measurement to provide this functionality. When a system starts its booting up process, the TPM checks for the different hardware, software and/or firmware components and runs an integrity measurement check on them to ensure that the system was not tampered with or changed before the startup process. The trusted boot is used to ensure the integrity of the monitored environment, both for cloud tenants and providers.

- Cryptographic operations: Included in the TPM is a coprocessor that handles cryptographic operations such as hashing, random number generation, asymmetric encryption, and key generation, that can be used directly or for several other purposes. All cryptographic operations on the TPM are hardware-based and use the SHA1, HMAC, and RSA algorithms.

- Secure authentication and communication: TPM in 5irechain can be used to authenticate a system and to secure communications between two entities. The TPM, being a root of trust, can authenticate a system when other entities request it, as the hardware of the TPM is certified through a certification authority. For communications, the TPM, through its AIK pairs, can help establish a secure channel so that information can be exchanged between two entities.

- Identification: Through the TPM, it is possible to uniquely identify 5irechain's user. A TPM has a single unique key, called the EK, and an embedded key pair unique to each TPM. This key pair also has a certificate associated with it, of which the public key part of the EK comprises. This certificate ensures that the TPM conforms to specifications. However, it is rarely used to verify the TPM. This falls on the AIKs that are generated from the EK. The AIKs can then be used to verify the identity of the user of that specific TPM.

- Data protection: TPM deals with 5irechain's remote attestation and integrity measurement of the streaming data. This assures the secure collection and transmission of forensic data from cloud services and prevents manipulation and falsification of the forensic data

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

- Detect unauthorized access: TPM could be used to detect unauthorized access. In the 5irechain architecture, TPM is emulated to provide trust management with hypervisor-level policy-based access control. This prevents the access of unauthorized users to the resources.

Processes……
1. All nodes (N1,N2...Nn) other than the proving node will generate a challenge nonce (CN1,CN2...CNn) and send it to the proving node for generating a fresh attestation claim. 2. Proving nodes will generate (CN1,CN2...CNn). 3. Proving node will ask TPM device to digitally sign freshly generated hash with current PCR values. 4. TPM will generate Signature, hash (pcr values), (CN1,CN2...CNn) 5. Proving nodes will send Signature, hash (pcr values), (CN1,CN2,CNn) along with actual challenge nonce sent by nodes (CN1,CN2...CNn) to be added to blockchain. 6. Challenging nodes will verify (Signature, hash (pcr values), (CN1,CN2,CNn)) by generatingthe new (CN1,CN2...CNn) to make sure that right challenge nonce was signed by the TPM.

4.0 KEY ESTABLISHMENT PROTOCOL, SYSTEM CONFIGURATION, AND OVERVIEW

The objectives of any cryptographic key establishment and management protocol are threefold:

- Establish a secure link between each node and the base station
- Allow for runtime key updates resulting from movement or addition/deletion of nodes
- Establish pairwise or group keys between subsets of sensor nodes. In this section, we will focus on the problem of establishing

We observe that a Stargate (TPM-enabled node) can establish a secure link with the base-station over the WiFi or Ethernet network using standard secure communication protocols such as SSL. Thus, we can reduce the problem of establishing a secure link between a Mote (non-TPM-enabled node) and the base station to the problem of establishing a secure link between the Mote and the Stargate.

The only pre-deployment configuration required by our protocol is a single asymmetric public-private key pair. The public part of this key, PUnetwork, is programmed into every Mote at the time of deployment. The private key, PRnetwork, is disclosed only to the TPMs. In order to achieve this, the base station sends this key as an encrypted key blob to the Stargates. The base station uses the public key of the TPM for generating this blob. Note that the base- station can gain access to the public key of the TPM through certifying authorities. The Stargate loads this key blob in the TPM, using the command TPM_ConvertMigrationBlob. The figure below presents an overview of the key establishment protocol between a Mote and a Stargate.

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

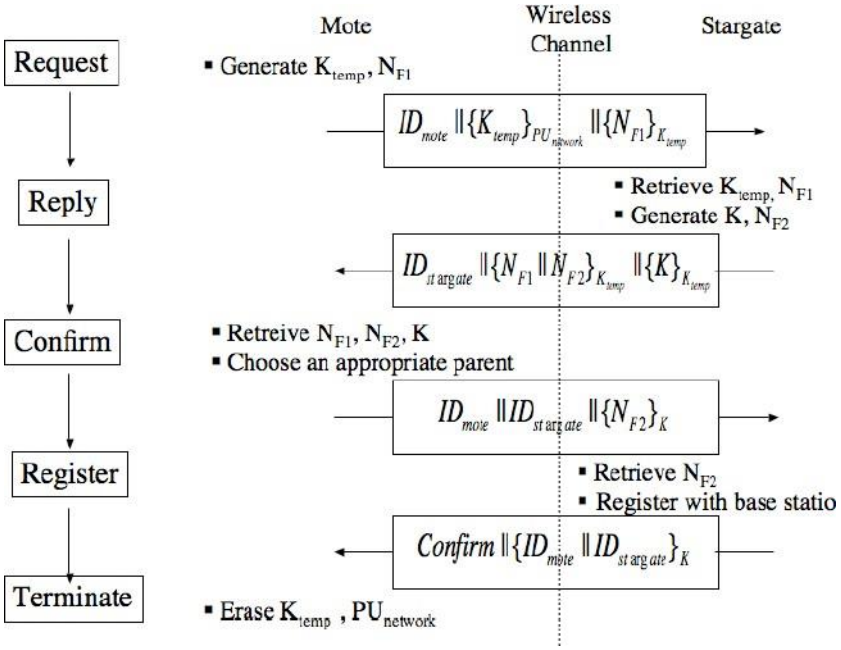


Figure 3: Key establishment protocol

Step 1: Request

As soon as a Mote boots up, it sends out a key establishment request. The specific actions that a Mote performs are explained below:

1. It generates a random number, NK, which is used for generating a temporary key, Ktemp, by taking a SHA-1 transform of NK, Ktemp = SHA-1(NK). A key blob is created for the temporary key by encrypting it with the network public key, PUnetwork.
2. The payload of the key establishment request packet contains the identity of the Mote, IDmote, a random freshness nonce, NF1, and the key blob containing the temporary key, Ktemp. The nonce safeguards against replay attacks as explained later in this section. The identity of the Mote is sent in plaintext, but the nonce is encrypted using the temporary key, Ktemp.

IDmote || {NF1}Ktemp || {Ktemp}PUnetwork

Here, {M}K represents that the payload M is encrypted using the key K and || denotes concatenation.

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

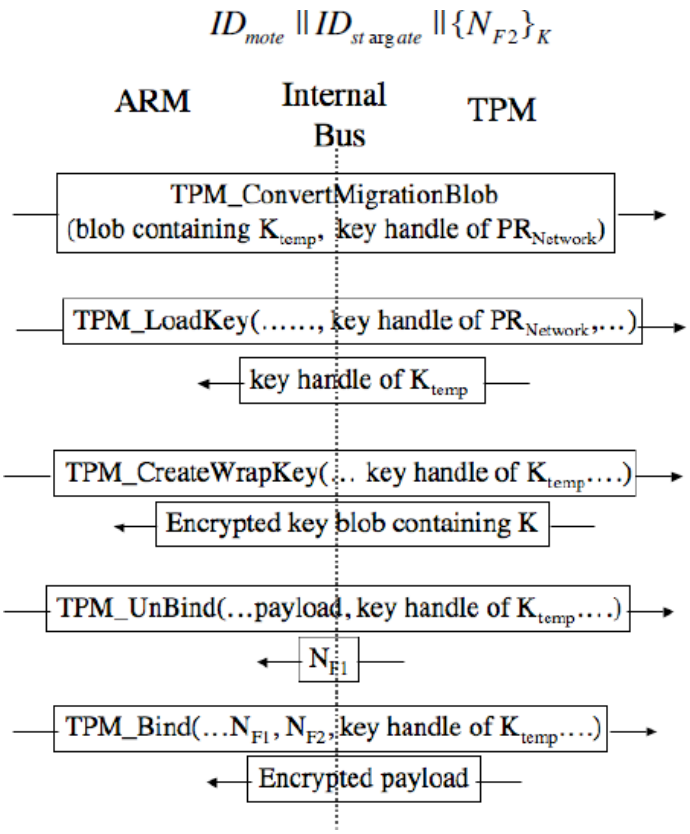


Figure 4: Interaction between ARM processor and TPM at the Stargate during key generation

Step 2: Reply

Upon receiving a key establishment request packet, the specific actions performed by the Stargate2 and the TPM are explained below (see Figure 3).

1. The Stargate uses TPM_ConvertMigrationBlob and TPM_LoadKey to import the temporary key, Ktemp, in the protected memory of TPM. The TPM returns the key handle of the temporary key to the Stargate.
2. The Stargate uses this key handle, as the parent key, to generate a new key for the Mote, represented by K(TPM_CreateWrapKey). The TPM returns the encrypted key blob to the Stargate containing K.
3. The Stargate uses TPM_UnBind to decrypt the second part of the payload and retrieves the freshness nonce, NF1. Following this, the Stargate creates a new freshness nonce, NF2, and uses the TPM_Bind command to encrypt the two nonces, NF1 and NF2.
4. Finally, the Stargate sends a reply packet to the Mote containing its identity, the encrypted nonces and the key blob containing the secret key.

IDStargate || {NF1 || NF2}Ktemp || {K}Ktemp

Step 3: Confirmation

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

1. The Mote decrypts the reply packet to retrieve the freshness nonce, NF1. The validity of the freshness nonce has two implications. First, it verifies the authenticity of the replying Stargate. Only a valid Stargate, using a valid TPM, could have been able to decrypt the key establishment request and retrieve the temporary key, Ktemp, from it. Second, it safeguards the Mote from replay attacks. Every new key establishment request from the Mote will contain a new freshness nonce, which can help the Mote differentiate between fresh and stale replies.
2. The Mote randomly chooses one of the Stargates with a valid reply to be its cryptographic parent. This choice can be made on the basis of network layer attributes such as link quality, hop distance etc. In our current implementation, we use a simple first-come first-served policy for making this decision.
3. The Mote then sends back a confirmation packet containing its id, IDmote, the id of the chosen cryptographic parent, IDstargate and the second freshness nonce, NF2 from the reply packet. The freshness nonce is encrypted using the secret key from the reply, K.

Dmote || IDstargate ||{NF2}K

Step 4: Registration

1. On getting a confirmation packet, the Stargate first imports the secret key, K, and then decrypts the payload using TPM_UnBind. The TPM returns the freshness nonce, NF2, to the Stargate. The validity of the freshness nonce ensures the Stargate that a secure communication path has been established between itself and the Mote.
2. The next step for the Stargate is to register the mapping, {IDmote, IDstargate, K}, with the base- station. As we will show in later sections, storing this mapping at the base station is critical for establishing a new secure path between the Mote and the base station. However, to export the secret key, K, outside the TPM, it must first be converted into an encrypted key blob.
3. The Stargate generates this key blob using the TPM_CreateMigrationBlob command. The parent key used for encryption is the public key of the base station, so that only the base station can retrieve the secret key, K. Note that TPM can obtain the public key of the base station through trusted certifying authorities. On receiving the key blob from the TPM, the Stargate sends the key blob along with the tuple {IDmote, IDstargate} to the base station.
4. Following this, the Stargate sends a registration packet to the Mote to trigger the termination of the protocol.

Volume: 05, Issue: 03 " May - June 2022"

ISSN 2582-0176

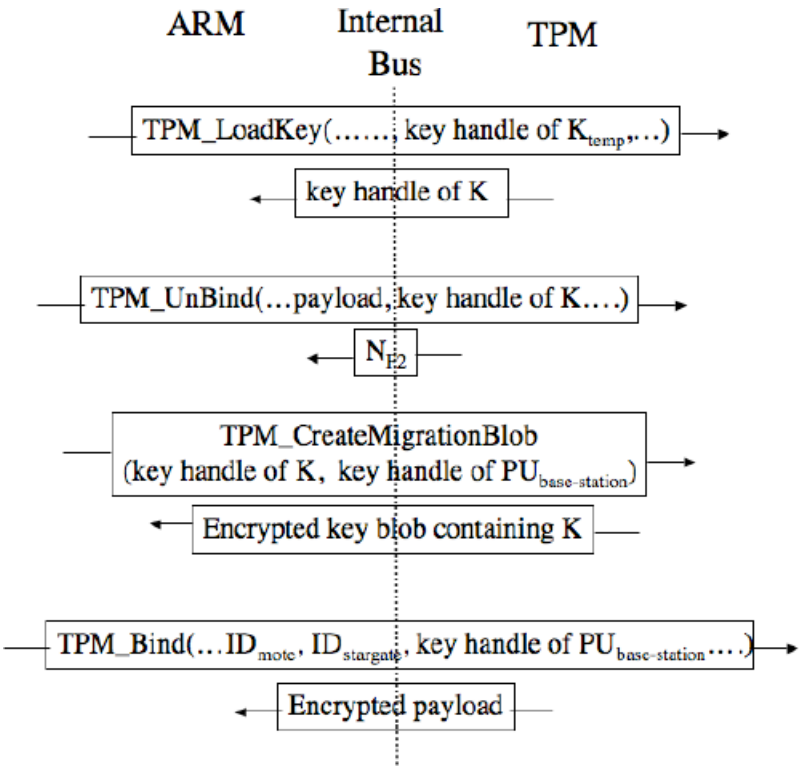


Figure 5: Interaction between ARM processor and TPM at the Stargate during key registration

Step 5: Termination

Upon receiving the registration packet, the Mote is assured that a secure communication path has been established to the base station via the Stargate. Following this, the Mote erases the network public key, PUnetwork, and the temporary key, Ktemp, from its storage. If a Mote does not get back a reply within a stipulated amount of time, it performs the following actions in the specified order: (1) Resends the confirmation packet and waits for a reply, (2) Chooses another cryptographic parent and reruns the protocol from step 3, (3) Restart the whole protocol from Step 1.

5.0 CONCLUSION

Trusted platform modules (TPM) have become important safe guards against a variety of software-based attacks. By providing a limited set of cryptographic services through a well-defined interface, separated from the software itself, TPM can serve as a root of trust and as a building block for higher-level security measures. Sincerity and security concerns of 5irechain with using HRT to fill in that gap by being integrated with smart contracts. Thus, the main focus was to research how trusted hardware like Trusted Platform Module (TPM) can protect the execution of smart contracts. Preparation has been done for this research by doing a literature review and exploring various coding and benchmark tools for a prototype.

REFERENCES

Perrig, R. Szewczyk, V. Wen, D. culler, D. Tygar. SPINS: Security protocols for sensor network. Wireless Networks Jounral, 2002.

Bahga, A., Madisetti, V.K., Blockchain platform for industrial Internet of Things, J. Softw. Eng. Appl. 9(10), 533 (2016)

Boohyung Lee, Jong-Hyouk Lee, Blockchain-based secure firmware update for embedded devices in an Internet of Things environment, The Journal of Supercomputing, Volume 73, Issue 3, March 2017

Boudguiga et al, Towards Better Availability and Accountability for IoT Updates by means of a Blockchain, 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France

Endpoint Security: Hardware Roots of Trust," by Derek Brink, June 2012. http://www.aberdeen.com/Aberdeen-Library/7080/RA-trusted-computing-security.aspx

Internet of Things, IEEE Access, V. 4, 2016

K Christidis, M Devetsikiotis, Blockchains and Smart Contracts for the

Kouzinopoulos C.S. et al., Using Blockchains to Strengthen the Security of Internet of Things. Security in Computer and Information Sciences. Euro-CYBERSEC 2018, vol 821. Springer, 2018

S. Basagni, K. Herrin, E. Rosti, and D. Bruschi. Secure pebblenets. In Proceedings of ACM MOBICHOC. 2001.

S. J. S. Zhu, S. Setia. LEAP: Efficient security mechanism for largescale distributed sensor networks. ACM CCS. 2003.

Safenet, a TCG member, is the supplier of HSMs to Amazon Web Services (AWS), which announced the CloudHSM product in April of 2013. http://aws.amazon.com/cloudhsm

Shepherd et al, Secure and Trusted Execution: Past, Present, and Future - A Critical Review in the Context of the Internet of Things and Cyber-Physical Systems, 2016 IEEE Trustcom, Tianjin, China

SJ Johnston, M Scott, SJ Cox, Recommendations for securing Internet of Things devices using commodity hardware, IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 2016

TCG, "How to Use the TPM: A Guide to Hardware-Based Endpoint Security, http://www.trustedcomputinggroup.org/resources/how_to_use_the_tpm_a_guide_to_h ard warebased_endpoint_security

Trusted Computing Group: http://www.trustedcomputinggroup.org/

