Open Access License Notice

This article is © its author(s) and is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). This license applies regardless of any copyright or pricing statements appearing later in this PDF. Those statements reflect formatting from the print edition and do not represent the current open access licensing policy.

License details: https://creativecommons.org/licenses/by/4.0/

Best Paper Award 2016

Encryption at Birth through Trusted Platform Modules

Waldemar Pabon
waldemarp2011@hotmail.com

University of Maryland University College
3501 University Blvd. East
Adelphi, MD 20783 USA

Abstract - When looking at the next generation of trusted computing initiatives, secure packet content has to be one of the main concerns. The optional nature associated with securing the information in the packets, in conjunction with the risks associated with malware and hackers has to force the industry to move to an "encryption at birth" approach (packet structure should implement encryption) that should be an integral part of the out of the box design as opposed to a commodity. In this paper, we will introduce the recent research in the use of Trusted Platform Modules (TPMs) 2.0 as the main vehicle to encrypt packets communing out of network interface controllers (NICs) and have the routers incorporate the TPMs to provide packet deciphering, remote attestation, TPM Quarantine and serve as the central processing unit of a secure packet delivery Infrastructure.

Author Note

I would like to thank Jerry James for his fruitful insights and challenges which helped polish the final architecture of this research. Jerry was always there to ask the right questions which helped drive my efforts to those features that added real value to my work.

Keywords

Trusted Platform Module, Encryption, Remote Attestation, Secure Packets, Trusted Store.

1. INTRODUCTION

Protecting data confidentiality and integrity is everyone's business. And it becomes a major issue when one injects malware and hackers into the technology infrastructure equation. The industry has been able to respond by providing multiple tools that can be used to protect the information within a local area network (LAN): Virtual Private Networks, Secure Socket Layer certificates, firewalls, etc. Each requires a level of particular knowledge in order to properly implement the solution. But the fact associated with the optional nature of all the tools and capabilities provides an open door to compromise business most precious asset: information. Quantifying the cost of data breaches is an imperative exercise that will expose how fragile a technology infrastructure can be, even with all the available tools that exists today. Especially if we switch our attention to network packets and realize how the data that flows through any LAN is exposed by its very nature.

There has to be a change in paradigm; we must start to realize that in order to secure the packets when transferring the data through the local area network, it has to be encrypted by design and not as an optional approach. And we cannot pretend to make it happen only if a business implements one of the current available options out there in the market, because then an unfair advantage is created for those who know how to follow the best practices and those who don't (businesses that may lack the required expertise, guidance or the budget to do so). When looking at the whole picture, businesses and organizations face a big challenge when they have to maintain trained personnel, the proper hardware, the right software, real estate to host the hardware and any licensing requirement imposed by the selected approach to be used when securing the packets in the perimeter.

In any local area network that is exchanging packets in their raw format, it only takes one weak link to compromise the whole technology infrastructure. For the packets to be secure, the encryption needs to take place right at the point where the data is getting created and is ready to be transferred; the communication channel. This leads to the realization of the "encryption at birth" concept, which implies

that the packet itself needs to provide the encryption, as part of a new paradigm to handle secure packet distribution in a novel out of the box implementation.

In this paper, I propose a new type of architecture that will secure packets in the communication channel by design, from source to destination. I introduce three new components that will require to change the way the Network Interface Cards as well as the packet distribution devices (routers, switches, hubs and firewalls) are manufactured. A novel packet structure offering payload obscurity is presented in this research in order to support the packet encryption and a secure distribution process. Finally, a new component (a Trusted Store) that will serve as the central command and control vehicle for the design is introduced and explained. And in order to achieve this level of security with this new architecture, the Trusted Platform Module (TPM) 2.0 plays an integral part of this revolutionary packet exchange architecture. The main reason why the TPM is included with the solution relates to the fact that it implements tamper-resistance techniques to prevent a wide range of physical and hardware-based attacks [1].

2. RELATED WORK

Many colleagues have researched Trusted Platform Modules (TPMs) and their application to different architectures within the trusted computing landscape in order to provide secure channels when distributing digital information. In Hao, Yu, Qianying, & Shijun [3] research, for example, they proposed the use of Trusted Platform Modules as a mechanism to secure the distribution of digital content in a peer to peer network communication (no router existence to manage the delivery), leveraging the tamper-proof nature of the TPMs.

Zhou, & Zhang [5] on the other hand, proposed a Password-based authenticated key exchange protocol to be used in conjunction with the TPMs in order to establish secure channels and protect the data transfer. Their work also presents a concept that is of real importance to our new design, which is maintaining a secure channel when performing attestation. This approach is vital to prevent other devices from intercepting the data transfer and replaying the messages while making modifications at it (Man in the Middle attacks).

Finally, strategies to establish a secure tunnel endpoint through TPMs have been also researched in the past. Goldman, Perez & Sailer [2] work regarding secure tunneling endpoint through remote attestation provide some insight as to how can any business leverage the TPM Attestation Identity Key (AIK) capability to secure the endpoints in any communication.

But when we take a look at all the alternatives that are within reach, we are missing a cohesive design for packet distribution in the LAN that could handle secure packets by itself at the hardware level without the need of additional pieces of software. Instead, we see organizations and businesses alike investing in securing their packets as they are transferred in the communication channel. And they are forced to get involved in the maintainability of different secure data solutions (PKI infrastructure, IPSec, etc.) with the additive requirement of high end expertise for the technical personnel, plus the time that must be spent to secure the infrastructure and master those solutions. Businesses should really invest in technology to convert the information infrastructure into an asset that will help achieve efficiency and add value to their operations; instead of converging on a cost center approach. With this concern in mind, a new secure packet distribution architecture is created and presented as part of this paper.

3. NEW PACKET STRUCTURE

In order to support the proposed architecture in this paper, a new packet structure is required in order to handle a secure communication in the local area network. I propose a novel design that incorporates encryption as an integral part of the packet structure itself in order to provide obscurity to the packet data (header, payload and footer). The new packet structure will contain two main sections as part of its format: header and encrypted payload (see Figure 1 below).

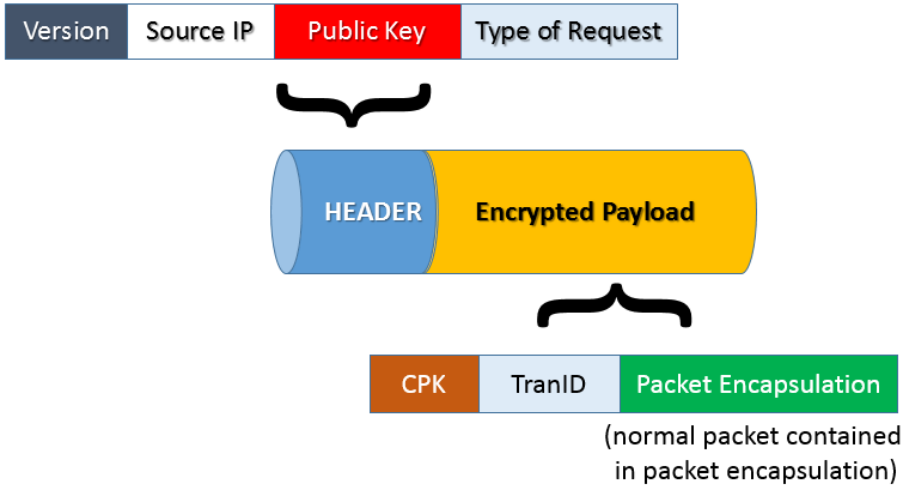

Figure 1: New Packet Structure

The header section is composed of four main components: version, source ip, public key (PK) and the type of request (ToR). Table 1 summarizes the characteristics and use of each field in the header section.

Table 1
New Packet Structure – Header Section

Field	Description
Version (required)	Version of the new packet structure.
IP Address (required)	The IP Address of the requesting endpoint.
Public Key (PK) (optional)	Public Key used to encrypt the payload of the packet depending on the step in the packet distribution process. This represents the shared secret to be distributed to the endpoint form the Trusted Store.

Table 1
New Packet Structure – Header Section

Field	Description
Type of Request (ToR) (required)	This will signal what type of request the endpoint needs to manage. This field will manage the following types: ▪ Communication Request (CR) ▪ Attestation Challenge (AC) ▪ Attestation Response (AR) ▪ Communication Request Acknowledgement (CRA) ▪ Packet Distribution Request (PDR) ▪ Packet Delivery Intent Acknowledgement (PDRA) ▪ Packet Delivery (PD) ▪ Delivery Acknowledgement (DA) ▪ Delivery Confirmation (DC)

The fields contained in the header section provide the minimum amount of data necessary to initiate the packet distribution process and without exposing details that could be used to attack the confidentiality of the information.

The new encryption payload section provides the necessary obscurity in the communication channel to maintain the confidentiality of the data, the destination and all the internal controls that are in place to maintain a secure and stable packet distribution process in the LAN. The encryption payload section is composed of three main fields: communication public key, transaction id and packet

encapsulation. Table 2 provides a summary of the fields and their characteristics in the new packet structure.

Table 2
New Packet Structure – Encryption Payload Section

Field	Description
Communication Public Key (required)	This public key is generated at the Trusted Store, utilizing the TPM in order to create a unique public key for each communication against each endpoint.
Transaction Id (required)	A random transaction id generated by the Trusted Store to identify the particular packet distribution process in its internal registry.
Packet Encapsulation (required)	Packet encapsulation provides a wrapper for the currently existing packet formats, but accommodated within the encrypted payload structure.

One of the important aspects of the encryption payload is the fact that a new communication public key is generated for the source endpoint when a new payload is ready to be transferred as well as for the communication that is initiated from the Trusted Store (a new component in charge of the secure packet distribution process) to the destination endpoint. This dynamic has the main objective of preventing that compromising a single communication could jeopardize the new architecture. The Trusted Store will use the TPM cryptographic capabilities at the packet distribution device in order to produce two public keys per communication; one for the source and one for the destination. Another

important aspect is the random transaction id that is associated with each communication initiated at the source endpoint. This transaction id will be used by the Trusted Store to keep track of the packet delivery process. Finally, encapsulating the current packet structure used by the different protocols will allow the distribution process to be able to perform as expected without suffering major changes.

As it can be appreciated from the new packet structure, the Trusted Platform Module (TPM) 2.0 capabilities are leveraged in order to support the new proposed architecture. It is because of the TPMs that the public keys can be generated and shared in addition to the attestation process, which will be used to make sure that the valid TPMs only are allowed to communicate in the infrastructure.

4. TRUSTED STORE

The Trusted Store is a new component that must be implemented at the packet distribution device level (routers, hubs, switches, firewalls, etc.). Due to its basic nature in controlling the packet exchange process, this component needs to account for six (6) important functions as illustrated in Figure 2.

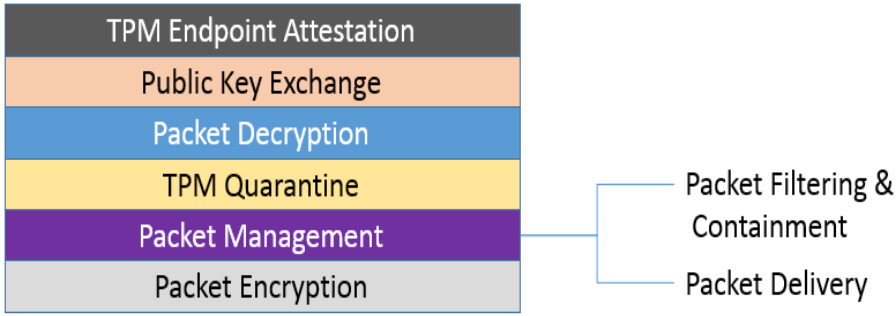

Figure 2 Trusted Store Functions

4.1 TPM Endpoint Attestation

In order to have a secure communication, we need to make sure that the endpoint that will be transmitting information is a valid entity. That is the sole

responsibility of the TPM Endpoint Attestation function. This function uses the attestation capabilities of the source TPM [4], in order to maintain an internal registry of all the TPMs that could be communicating over a secure channel at any given point as long as the Trusted Store can attest the endpoint. Here, the Platform Configuration Register (PCR) is used to evaluate if the corresponding TPM belongs to the corporate network and has loaded all the required components for the client to participate in the packet exchange process. The registry generated from the TPM Endpoint Attestation function in the Trusted Store can be accessed by an administrator of the packet delivery device in order to be able to change the operational status of each TPM in the LAN. The packet delivery device will maintain a relationship of PKs, Transaction Ids and IPs, which will be used to cross reference which packets can securely flow in the network along with valid TPMs.

From an attack perspective, this will allow administrators to be able to manage / control which endpoints should be allowed / disallowed in the communication channel. This kind of control will provides a useful tool that can stop attacks coming from a compromised Trusted Platform Module at any given point, isolating the offending TPM from the local area network. Any threat attempting any kind of attack will have to replace the Network Interface Card with a new one (containing a new TPM every time) when moved to quarantine in order to try to initiate a new attack. And due to the restrictive nature of the Endpoint registry, an administrator can choose to only allow known TPMs (including the attestation required), which will also prevent foreign TMPs from getting access to the network.

4.2 Public Key Exchange

To ensure that repetition is not included in the encryption / decryption process, the Trusted Store will generate a new public key for each communication request using the TPM cryptographic capability; that is, one public key for the communication between the source endpoint to the Trust Store and another public key for the communication originating from the Trust Store to the destination endpoint. This function will exchange the public key required by the TPM to be used during the encryption process of the packets at the source endpoint as well as

a new public key to be used for the decryption process of the packets at the destination.

4.3 Packet Decryption

Once the source endpoint receives the public key to be used for the encryption process, stores it as part of the keys in the TPM and it uses that same public key to encrypt each packet of a particular communication, creating the new packet structure that hold the transaction id and the encrypted payload. The Trusted Store will receive the new packet structure and will use the private key associated with that particular communication to decrypt each packet from the source endpoint using the TPM capability (leveraging *TPM2_RSA_Decrypt*). During the decryption process, the normal structure of the packet that resides in the packet encapsulation section is exposed: header, payload and footer. At this point, the packet distribution device can check the packet header and determine its destination, type of data to be transferred, etc.

4.4 TPM Quarantine

The Quarantine function is used whenever an unrecognized TPM or a compromised TPM is found trying to transmit data over the local area network. This function pretty much filters out any packets coming out of a not authorized TPM in order to prevent those packets from flooding the network and waste resources unnecessarily. To do that, the Trusted Store uses the Endorsement Key Public Key (PK) of a TPM that is transferred as part of the encrypted payload and leverages the unique nature of it (since each manufacturer burns the PK directly to the TPM chip). The administrator will have the option to add / remove a TPM from the quarantine area as soon as that device is either compromised or clean / fixed. This function will have an alert capability that can generate a communication to the administrator in order for him / her to take immediate action (allow / deny access). The default behavior of this function is a default deny approach; prevent access from TPMs unless otherwise specified.

4.5 Packet Management

After the packet gets decrypted at the Trusted Store, the packet management capabilities can be used. The packet management function is responsible for inspecting the destination, validating that the source is not a compromised TPM, dropping any packets that are not coming from a valid source, handling errors and route encrypted packets to destination through the appropriate route. Depending on the type of packet distribution device, the route process can change (hub delivery versus router delivery), but the overall distribution approach will push the new packet structure through the communication channel.

4.6 Packet Encryption

Once the Packet Management function determines that a packet can be delivered, it uses the packet encryption function to secure the packet information to be sent over to the destination endpoint. The packet encryption function is leveraging the TPM cryptographic capabilities by generating two important artifacts. First, a public key is created and included in a new packet that will be sent to the destination by the packet management function. The second artifact is a newly encrypted packet (leveraging *TPM2_RSA_Encrypt*), which will be delivered to the destination by the packet management function. This new packet is encrypted with the newly created public key that was shared with the destination endpoint TPM, along with the transaction id associated with the registered communication.

5. ENDPOINT TPMS

The endpoints, both source and destination, play an important role in the new architecture when trying to fit within the secure communication strategy. First, the source endpoint will use its TPM to provide the Endorsement Public Key that will be used by the Trusted Store to encrypt the communication public key to be used by the source endpoint. On the other hand, the destination TPM will be used in a similar strategy against the Trusted Store when decrypting the packets.

Even though the TPM has been added traditionally to the motherboard of new computers, in this new architecture they are actually added to the NIC cards. The

whole reasoning is because of migration purposes: it will be easier and a better cost effective solution to replace a NIC card in an old computer that has no TPM as part of its motherboard, than replacing the whole motherboard. This will make the transition to the new architecture a more affordable solution from a migration as well as budget perspective.

6. New Trusted Computing Architecture

In order to understand the new proposed trusted computing architecture, it is imperative to review the traditional communication process that takes places whenever a device is trying to transfer data from one endpoint to another in the LAN. When a computer initiates the data transfer, the information is broken down in packets that are transferred over an Ethernet connection and those packets get communicated by a hub, switch, router, or any other piece of hardware (see Figure 3). The challenge with the traditional implementation is that packets represent raw pieces of data that anyone can trap and even modify (unless optionally protected using different tools).

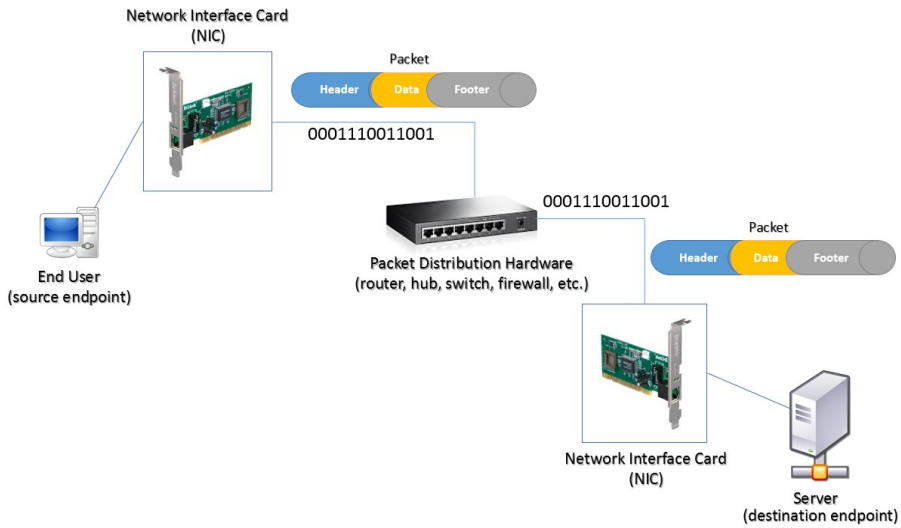

Figure 3 Packet Raw data getting transferred from one endpoint to another

In order to solve the raw nature of packets, we need to be able to encrypt the data right at the NIC card serving as the source endpoint, keep it encrypted through the entire packet distribution channel all the way down to the destination endpoint NIC at the hardware level. To achieve this, the Trusted Platform Module plays a major role as part of the new proposed architecture.

For the new architecture to be secure and trusted, we need to incorporate the TPMs as part of the source endpoint NIC, the packet distribution hardware (router, switches, hubs, firewalls, etc.) as well as the destination endpoint NIC card. Both endpoints will leverage current TPM capabilities in order to handle the new packet structure and provide public endorsement keys that will be used during the encryption process. The packet distribution hardware will also need a TPM because of the new responsibilities that this device will acquire as part of the new Trusted Store component.

In essence, the newly proposed communication architecture will require several important milestones to be achieved in order to maintain a secure communication in place: TPM attestation, public key exchange and obscurity (the most important component) in order to protect the packet information. Keeping the data "secret" and only available on a "need to know basis" will definitely help guard against any attacker trying to get access to the information; maintaining this way data confidentiality and integrity.

The following events provide an understanding on how the new packet distribution process will work under the ruling of the Trusted Store:

- **Step 1**: Source Endpoint (se) will initiate a Communication Request (cr) against the Trusted Store. At this juncture, the source endpoint will share its public key (PK) with the Trusted Store in order to use it when encrypting the token to be used for the communication that will take place between the source and the destination. This PK is part of a set of public keys that will get generated by the NIC card as soon as the device loads.
- **Step 2**: Attestation Challenge will take place depending on the setting at the Trusted Store. The attestation challenge has two basic settings for the administrator to choose from: aggressive or passive. The aggressive attestation

will occur on every communication while the passive will take place on a defined schedule.

- Step 3: The source endpoint TPM will use its Endorsement Key as a finger print process to attest its validity, and the Trusted Store will validate the endpoint TPM and update its internal table to keep track of which TPMs are authorized or not to transmit data in the network. If the endpoint TPM cannot be attested, the packets from the endpoint will be dropped as soon as they are received.
- Step 4: Using the PK from the source, the Trusted Store will send a packet to the source endpoint with an encrypted payload. The encrypted payload will contain the transaction id to use for the authorized communication as well as the communication public key (CPK) to use when encrypting the payload at the source endpoint (generated through the TPM cryptographic functions). The Trusted Store will use asymmetric encryption to secure the encryption payload.
- Step 5: Source Endpoint will send the encrypted payload containing the transaction id for the communication as well as the packet encapsulation (which hold any current packet format). The encrypted payload is created using the received public key from the Trusted Store during Step 4.
- Step 6: Attestation Challenge is performed against the destination TPM. The same validation performed at Step 2 is executed also in this step.
- Step 7: The destination endpoint (de) TPM will attest its state, Trusted Store will validate the state of the endpoint. This is the same process as Step 3; in this case the destination TPM is involved.
- Step 8: The Trusted Store shares the Communication Public Key for the destination endpoint. This will be used to transfer the destination PK to be used by the Trusted Store when sending down the packet for decryption at the destination endpoint.
- Step 9: The destination endpoint encrypts his PK to be used by the Trusted Store when sending the encrypted payload (transaction id + encapsulated packet).
- Step 10: Trusted Store sends the packet and the transaction id to the destination endpoint. The destination will use the transaction id to communicate the acknowledgement back to the Trusted Store.

- **Step 11**: Destination Endpoint sends the acknowledgement to the Trusted Store indicating that the packet delivery is complete.
- **Step 12**: Trusted Store sends the acknowledgement to the Source Endpoint indicating that the packet delivery is complete.

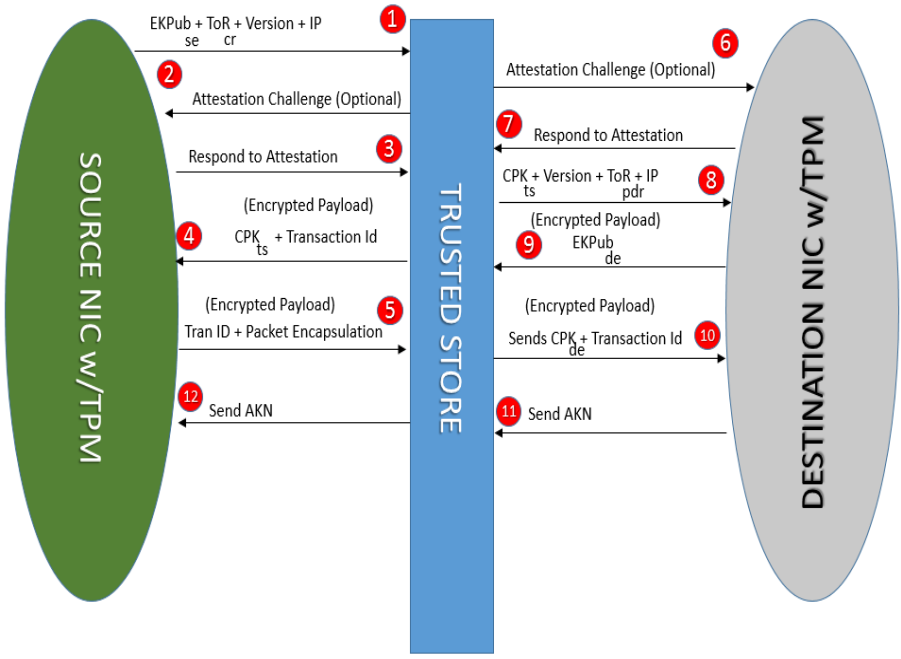

Figure 4 Secure Communication through TPM Trusted Store

Since the state of the endpoints can get compromised at any point during the lifecycle of the communication process, the aggressive option related to attestation is used to ensure that the state of the endpoint TPM is ok in order to update its state in the Trusted Store registry. This validation process will support the quarantine and the packet management functions. One important aspect of the new proposed architecture is the fact that it's leveraging existing features in TPMs.

7. BENEFITS

There are several direct as well as indirect benefits achieved through the new architecture. The benefits have a broad spectrum range; from data confidentiality, technical knowledge requirements to cost reductions.

7.1 Data Confidentiality and Integrity

Encryption as the principal component of the new architecture is used to make sure that packets (header, payload and trailer) are secure as soon as they enter the physical layer. The obscurity nature of the packets limit the capability of attacks (such as Main in the Middle) from getting any piece of information out of them; using tamper-resistant hardware that could be easily quarantined by administrators in case any of the TPMs get compromised. This benefit is tightly coupled with the protections offered by the new architecture to safeguard data confidentiality and integrity.

7.2 Technical Skills

Due to the natural integration of encryption as part of the data packets, there is no need to acquire or maintain any kind of special technical skill to secure the data that is flowing in the local area network of any organization or business. This means that the need to maintain SSL certificates, PKI servers, VPN tunneling, etc. internally and all the technical knowledge associated with this is not relevant anymore. The new architecture simplifies the composition of the IT infrastructure and allows for the natural components to be secure by design; achieving encryption at birth through the communication channel. The IT personnel can now spend their time in other important tasks of the business without having the collateral risk of not knowing how to secure the packets in the network. This is one of the main advantages of this architecture since now security becomes an integral part of data communication instead of a commodity.

7.3 Hardware and License Costs Savings

There is an immediate cost reduction effect associated with hardware and licenses. The fact that now the packets are secure "at birth" is a good justification

to lower down the cost for any hardware or licenses associated with any legacy approach used to maintain a secure communication channel in place in the local area network. The physical hardware can be decommissioned or even re-purposed. If decommissioned, there is an immediate utility cost reduction as well as a real estate gain that is also achieved since the physical server has no need to consume electricity or even occupy data center real estate.

7.4 Streamlined Security Infrastructure

When combining the reduction in technical skills knowledge required for the maintenance of the legacy security approaches, plus the reduction in licenses, the removal of those two elements alone pretty much simplify the security infrastructure mix. That is achieved due to the fact that we gain a reduction in the complexity of the required components to secure the data in the communication channel. This streamlined infrastructure is achieved by the design of the new architecture, providing businesses with the opportunity to concentrate their efforts in things that add value to the operation as opposed to incur in costs associated securing their data.

7.5 Virtualization

The scope of the encryption achieved through the TPMs in the NICs also benefits not only server, but client virtualization as well. When we look at the strategy behind virtualization, the sharing of hardware, in this case the NIC containing the trusted platform module, will allow multiple instances to run under the same encryption strategy. This has a huge cost reduction impact since multiple virtual machines can maximize the cryptographic functions of a single TPM.

8. FURTHER DISCUSSIONS

At the inception of computer systems, security was not a big concern. With innovation, it became clearly evident that security as a basic ingredient to the computer systems design process was greatly overlooked. This means that the industry was forced to compensate for the exclusion of security at the design level and great minds provided alternate solutions for the security challenges that

businesses were facing when trying to protect confidentiality, integrity and availability of the information.

Putting this issue into context against the new architecture I'm presenting as part of this research, there is a great amount of hardware that already exists out there in the world that is not accounting for the requirements of the Trusted Store. This means that migrating routers, switches, hubs, etc. that could support this would require a good amount of budget consideration (in contrast to new network implementations which can have the advantage to implement a secure communication strategy from scratch).

From the Trusted Store perspective, the fact that already existing NIC cards may not incorporate TPMs to be able to send encrypted packets creates the burden of either allowing a duplex function at the Trusted Store (to be able to handle encrypted as well as not encrypted for legacy hardware) or not allowing the not encrypted communication at all. From a flexibility standpoint, everything will point at the fact that maintaining a duplex capability will account for legacy networks while they transition into the new secure architecture (NICs with TPMs), but at the expense of dealing with the well-known attacks and security vulnerabilities associated with raw packet data.

Finally, since we are achieving a secure communication between the endpoints where no one has access to the raw data in the packets, the endpoints themselves become a more attractive target of attacks. We removed the risk from the networks communication, but now created a new risk at the endpoint level. This fact stresses the importance of focusing our efforts to secure the endpoints better, to help maintain data confidentiality and integrity.

9. CONCLUSION

With the intention of creating a secure communication exchange that is incorporated as part of the network communication design and not as a commodity, the encryption at birth strategy is included as part of the new secure packet distribution architecture presented in this research. This paper leverages Trusted

Platform Modules 2.0 capabilities that already exists and deal with encryption as an integral part of securing the packet distribution process. The new architecture is designed to account for control mechanisms that can be used to prevent or contain the compromise of data confidentiality and integrity, achieving a secure exchange of information. The Trusted Store along with the encryption capabilities of the TPM provide strong evidence for the feasibility of "Encryption at Birth" as an out of the box implementation; either with new or existing local area networks.

Finally, the encryption at birth achieved through the hardware without the need to implement a PKI infrastructure or configure IPSec protocols, for example, is the biggest contribution of this novel process. This means that the responsibility of ensuring confidentiality and integrity is achieved by default without the requirement of additional tools or high end knowledge. From an attack perspective, no network sniffing by any attacker will expose the packet payload information, preventing anyone from changing the contents of the packet, retrying packets or even performing Man in the Middle attacks because of the obscurity nature of the information. This proves that we can achieving "Encryption at birth", allowing data to flow secure in the communication channel as a normal integrated ingredient of the packet distribution process.

REFERENCES

[1] Aaraj, N., Raghunathan, A., & Jha, N. K. (2008). Analysis and Design of a Hardware/Software Trusted Platform Module for Embedded Systems. *ACM Transactions On Embedded Computing Systems*, 8(1), 8-8-31. doi:10.1145/1457246.1457254

[2] Goldman, K., Perez, R., & Sailer, R. (2006). Linking remote attestation to secure tunnel endpoints. Proceedings Of The First ACM Workshop On Scalable Trusted Computing, STC'06. A Workshop Held In Conjuction With The 13Th ACM Conference On Computer And Communications Security, CCS'06, (Proceedings of the First ACM Workshop on Scalable Trusted Computing, STC'06. A workshop held in conjuction with the 13th ACM Conference on Computer and Communications Security, CCS'06), 21-24. doi:10.1145/1179474.1179481

[3] Hao, L., Yu, Q., Qianying, Z., & Shijun, Z. (2011). Securing the Distributions in P2P Networks with Trusted Platform Modules. *International Journal Of Computer Network And Information Security*, (2), 26.

[4] Trusted Computing Group. TCG TPM Specification Version 1.2. Parts I-III, 2005.

[5] Zhou, L., & Zhang, Z. (2010). Trusted channels with password-based authentication and TPM-based attestation. *2010 WRI International Conference On Communications And Mobile Computing*, CMC 2010, 1(2010 WRI International Conference on Communications and Mobile Computing, CMC 2010), 223-227. doi:10.1109/CMC.2010.232