International Journal of Cryptology Research 4(1): 55 - 67 (2013)

Mutual Remote Attestation in IPSec Based VPN

[1,2] *Norazah Abd Aziz, [2] Sharipah Setapa and [1] Nur Izura Udzir

[1]Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia

[2]MIMOS Berhad, Technology Park Malaysia,
57000 Kuala Lumpur

E-mail: azahaa@mimos.my, sharipah@mimos.my and
izura@fsktm.upm.edu.my

*Corresponding author

ABSTRACT

Secure communication between computer systems is normally established using secure tunnel technologies such as Internet Protocol Security (IPSec). IPSec protocol guarantees authenticity of communication and secure the data at each gateway but it does not provide any assurance on the entity authentication. So, it is important to make sure the trustworthiness of the remote party that already has a faithful system. Trusted Computing Group (TCG) has introduced a platform to solve this issue into the mainstream computer industry through their main approach called Trusted Platform Module (TPM). TPM is a security module which has been designed to store information of system events securely as well as the key component in the attestation realization. Trusted Computing Platform (TCP) provides a mechanism to supports attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. Attestation is a mechanism to provide remote assurance of the state of the hardware component running on a computing device. This paper, proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation. An embedded attestation extension is provided in VPN communication such as IPSec protocol by establishing mutual properties based attestation using Internet Security Association and Key Management Protocol (ISAKMP) measurement value as properties that are computed from security policy database (SPD). Hence, the proposed approach will protect both sender's and receiver's platforms integrity at their respective gateways.

Keywords: IPSec protocol, Trusted Com, uting Group (TCG), Trusted Platform Module (TPM), Trusted Computing Platform (TCP), Platform Configuration Registers (PCR), security policy database.

1. INTRODUCTION

Virtual Private Networks (VPN) is a method to achieve secure network that are widely used over public network infrastructures. It offers the easy way to handle complex networks as well as maintaining sure data transfer between two network hosts. Similar to TLS, this security protocol protect data transmission by authenticating endpoints connection and promises the data integrity and confidentiality. However, the VPN mechanism acquires severe managerial restriction in order to provide the better perimeter security for all VPN endpoints. Hence, it affects the VPN secure capabilities to protect the network from attacker. Although, there are many proprietary security software solution such as anti-virus moving towards solving this issue but it still cannot prevent unexpected attacks. Furthermore, the complexities of the solution may reduce the interoperability of the mechanism with other software. Other than that, this protocol do not provide authentication of users' computers configuration. If the computer has been compromised, the attacker may be able to get unauthorized access to the VPN connection in organization's intranet.

Attestation is a mechanism to provide remote assurance of the state of the hardware component running on a computing device [1]. It provides the trust foundation for computing platform by achieving the integrity of properties and/or configuration of the platform. Remote attestation is a process by which a TCG compliant platform embedded with Trusted Platform Module (TPM) authenticates its platform to a remote platform by sending its hashes of the properties or configuration platform component via digital signature. Then, the remote platform will verify the trustworthiness of the platform with standard or enhanced attestation protocol accordingly. Through remote attestation protocol, the requestor or client can access the remote platform without revealing its identity while allowing the requestor to verify the integrity of hardware and software of the running remote platform. So, the requestor can decide whether or not to trust the remote platform's configuration. In order to achieve the goals, the TPM [2] is implemented as the key component in the remote attestation realization. TPM provides the essential safe memory and cryptographic operation ability for the protocol. It provides a mechanism that supports the attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. The PCR are meant to store the integrity measurement safely.

Normally, we have to setup configuration before any communication is established. The configuration means any authorization mechanism such as username and password at the host. Since everyone can use the host, they can trace the username and password; hence change the configuration without notice by the owner of the host. Due to that, hosts lack the capability to remotely verify the hardware, operating system, or other software running. This leads to host vulnerabilities in operating system. TPM by using attestation approach, attempts to solve this deficiency using secure hardware and public-private key-pair as well as the module responsible in verifying the trustworthiness of the system.

Due to above limitations of VPN, this paper proposes IPSec key exchange protocol extension, using Internet Key Exchange (IKE). The extension embeds the attestation mechanism in IPSec protocol to ensure that only authenticated users using uncompromised platform is able to communicate in organization's VPN. Through this solution, the security of data will be achieved not only during network transmission but also on the involved endpoints in the VPN gateway. Furthermore, it can also prevent Man-in-the-middle (MITM) attacks since our approach provide secure linkage between the attestation and IPSec endpoint.

The rest of this paper is organized as follows. Section 2 discusses related work. Section 3 reviews about the IPSec protocol consist of IKE protocol flow. We demonstrate the framework of our approach in Section 4 and following is a details description on our IPSec extension with attestation. We discuss the security of our approach in Section 5. The paper ends with a conclusion.

2. RELATED WORK

The TCG has started Trusted Network Connect (TNC) project to utilize remote attestation in existing secure communication protocol. The TNC framework is discussed in [3] involving data exchanges between Agents [4][5] through network endpoints using attestation approach. In [6], the extended works of TNC method [4] that integrates with Extensible Authentication Protocol (EAP) framework was proposed. EAP is a protocol that enables multiple authentication mechanisms. However, this approach has a few issues which were discussed detail in [11].

The issue of compromised remote tunnel endpoints has been discussed in [7], but they focus on SSL implementation. They also proposed mechanism that links specific properties of a remote endpoint to gain TPM-based attestation. The approach focuses on virtualization environment implementation and aims to avoid certificate complexity. In [8], the author discuss about remote tunnel access tunnel involving VPN server. The paper focuses in depth of policy enforcement in order to verify the integrity of client properties. They introduced the method of track the changes of remote client's security properties by utilizing Linux prototype and attestation mechanism. However, they focus more on policy rather than embedded the attestation into IPSec architecture.

Other work which embeds the remote attestation in VPN has been discussed in [9][10][11][12]. In [9], they proposed Bound Keyed Attestation (BKA) that claimed to thwart the MITM attack. The BKA uses Diffie-Hellman key exchange during which each attestation endpoints derive a shared secret and prove to each other through both BKA's and IKE SA's shared secrets. Our approach differs in that we do not use Diffie-Hellman algorithm to perform attestation in IKE's phase 1 and phase 2.

The detail design and implementation of VPN architecture for trusted platforms was discussed in [10]. In the paper, they develop a prototype that provides access control and secure communication for arbitrary local compartment. Their latest paper [11] proposed new payload in IKEv2 named as Attestation Data Payload (ADP) in IKE version 2 to support various attestation protocols and architectures that is suited for remote attestation's future developments. Their approach's goals were to achieve simplicity and efficiency that claimed only minor changes to IKEv2 protocol and some extension has been made. Our method adopted and utilizes their approach which provides an embedded attestation extension in IPSec protocol but with different protocol flows.

A different solution is proposed in [12]. The solution utilizes configuration of the VPN to authenticate the user and establish VPN tunnel to perform a TNC handshake. The remote attestation is performed in the handshake. Then, the attestation's result is used by the Policy Enforcement Point to configure a packet filter. They claim that this approach is totally independent of the VPN solution, hence achieve interoperability. Unlike them, we use the policy during remote attestation. Other than that, they focus on to minimize customization and VPN components extension by proposed the new framework rather than embedding attestation in the IKE.

3. IPSec VIA INTERNET KEY EXCHANGE PROTOCOL (IKE)

Typically, users utilize a Virtual Private Network (VPN) to secure their network communication to their organization intranet from home, cybercafé and other places. The VPN offer security mechanism using cryptographic protocols in order to provide data confidentiality, entity authentication and data integrity. One of the security mechanisms is IPSec which developed by Internet Engineering Task Force (IETF). IPSec [13] is a protocol to provide end-to-end security in the Internet Protocol (IP) to secure and authenticate transmission of each IP packet of a communication session. IPSec consist of two main operations, namely Authentication Header (AH) and Encapsulating Security Payloads (ESP). AH is to protect against replay attack by offering data integrity and data origin authentication for IP datagram. ESP is also providing data origin authentication as well as data confidentiality and connectionless integrity. IPSec offers channel and transport encryption modes. The channel mode encrypt header and data payload but transport mode only encrypt the payload.

IPSec also provides Security Association (SA) [14] function in order to make use the AH and ESP. The SA is used as agreed security parameters between two communicating hosts for a secure tunnel. Each host can have multiple SAs to communicate with various remote hosts. The SA is identified through 32-bit Security Parameter Index (SPI). The SPI and the recipient IP address are used in order to index Security Association Database (SADB). The SADB contains many SAs which have different information about SAs that are distinguish by encryption algorithm, key and parameters, and lifespan of the SA. In order to establish an IPSec SA connection, both hosts need to exchange pre-shared key or public key certificates through Internet Key Exchange (IKE) protocol. The IKE is part of Internet Security Association and Key Management Protocol (ISAKMP) framework.

The Internet Key Exchange (IKE) [13] protocol is designed to perform mutual authentication through keys, algorithms and other attributes exchange of SA prior to establish IPSec channel. In this paper, we are concentrating on IKEv2 that perform authentication based on digital signatures adopted from [14]. The new feature of IKEv2 is that it always begins by negotiating the SA pair to establish an initial security association channel. The IKEv2 has two so-called exchanges phase. In the first phase, the users authenticate each other by exchanging nonce and performing a Diffie-Hellman key exchange protocol and establish an initial IKE security association (IKE SA). Then, in the second exchange, the users use the IKE SA to negotiate one or more AH or ESP security association between them. In other word, the cryptographic algorithms and keys used in each AH and ESP SA are negotiated to establish IPSec SA. In this phase, each host establishes the actual communication channel as child security association (Child SA) which is used to secure the subsequent IPSec channel. In [15], the authors extend the standard two exchanges phase of IKEv2 by one more phase called as extension. The [11] approach also defines the third phase as ‘info’ during which message transmission is encrypted with the IKE SA negotiation key. The message flow to establish IKEv2 is depicted in Figure 1.

Figure 1 illustrates the exchange message consist of nonce (N), Diffie-Hellman public keys (KEA,KEB) and negotiable attributes of the IKE SA pair (SA1A,SA1B) during the first phase, IKE SA INIT. The SA1A as example, contains A's crypto suite offers and SA1B B's preferences for IKE SA establishment. In IKE SA AUTH exchange phase, the shared secret KEAB is used to compute a session key SKAB. In this phase, each host need to authenticate the previous messages (AA, AB) and establishes a set of Child SAs (SA2A, SA2B). The Child SAs is used to negotiate the endpoint of the IKE SA that can also be used as actual data transfer. The computed session key then can be used as secure communication channel in the INFO phase.

IKE SA INIT			
1.	A -> B	:	$SA1_A$, KE_A, N_A
2.	B -> A	:	$SA1_B$, KE_B, N_B
IKE SA AUTH			
3.	A	:	$SK_{AB} = PRF(N_A \| N_B \| SA1_A \| KE_{AB})$
4.	A -> B	:	$enc_{SKAB}(A_A, SA2_A)$
5.	B	:	Validate A_A $SK_{AB} = PRF(N_A \| N_B \| SA1_B \| KE_{AB})$
6.	B -> A	:	$enc_{SKAB}(A_B, SA2_B)$
7.	A	:	Validate A_B
EXENSION INFO			
8.			$enc_{SKAB}(\ldots\ldots)$

Figure 1: Standard IKEv2 protocol flow

4. EXTENDING IPSec WITH REMOTE ATTESTATION

IPSec secure Internet Protocol (IP) communications by encrypting each IP packet of a communication session. However, IPSec only protects application traffic across IP network but not the integrity of the connection endpoints. Since this issue is not being addressed in IPSec, we propose to integrate remote attestation mechanism with IPSec.

Remote attestation is a mechanism for a remote party R to obtain assurance of the state of host V by authenticating V's measurement log against a stored value which is accepted as good state. V communicates with his TPM to sign a so-called TPM-quote containing the new R's nonce and current values of TPM's register (PCR) using private of Attestation Identity Key (AIK). V sends the measurement log and the quote to R together with the corresponding AIK certificate. The AIK certificate is obtained from Privacy Certificate Authority (PCA) [16], protocol proposed by the TCG that remotely convinces a communication partner such as that a piece of TPM hardware is trustworthy. R authenticates the AIK certificate using the PCA's public key and authenticates the quote using the AIK public key and his nonce. Then, R is able to authenticate the measurement log by using the authenticated quote. The authenticated log stated the integrity of host V securely to R. This paper proposed on properties-based attestation [17] means that emphasis on attesting behaviour of software component or properties of a platform. However we compute only the measurement value listed in the security policy database (SPD). This mechanism is known as property-based mechanism.

Before we describe our extended protocol in detail, we brief first about our framework. The framework containing the IPSec router with the embedded attestation illustrated in Figure 2. In the framework, each endpoint has built-in TPM capabilities in order to establish integrity measurement architecture and providing mutual remote attestation.

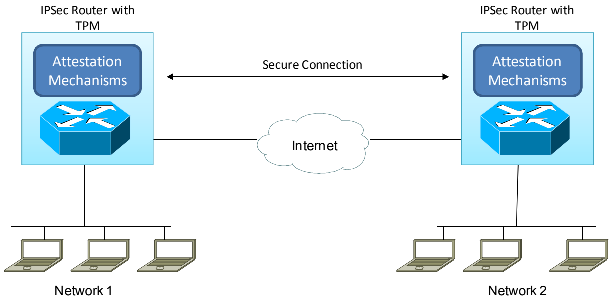

Figure 2: Mutual attestation between two network endpoints

Figure 3 depicts the relationship between IKE and IPSec with additional attestation approach. The Figure 3 shown that the IKE is an application layer protocol that using TCP/UDP to pass signal of IPSec protocol. The IKE negotiates SAs and transferred negotiated parameters and generated keys to IPSec for encryption and/or authentication of IP packets. In order to make security policy used in negotiation for attestation purposes, the IKE daemon need to be modified. The IKE daemon is integrated with the attester manager module to perform attestation mechanism. Since the security policy is used as integrity measurement for attestation, we must ensure the SAs perform same access security policy. The SA is unidirectional which means that each SA has to establish on inbound and outbound communication separately. For outbound communication, the modified IKE daemon ensures that any bundle of datagram retrieved matches the security policy. Otherwise, the SA can retrieve individually from the SPD to get same access security policy. The SPD is the database comprises of rules information for each IP packets within the network. So, the SPD is used to make decision on each packet of traffic determined by the rules. In our approach, we utilize this SPD to generate a core security policy that must be agreed upon registration.

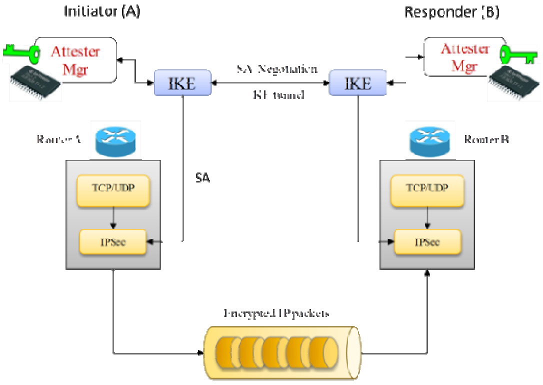

Figure 3: Proposed framework that shows relationship between IKE, IPSec and attestation

Basically, our method consists of three main processes: initial configuration process, remote attestation process and verification process. The initial configuration process is to generate the core properties based attestation hash value based on core policy and VPN configuration setup which has been agreed by each VPN endpoint. Remote attestation process as we know is involving authentication and negotiation process between each VPN endpoint. The last step is verification of encrypted data packet process.

In initial configuration process, a core policy based on VPN tunnel configuration that at least uses the IKE management service is generated. A core policy is generated based on system environment and requirement of each platform. The following steps show the process of obtaining the core integrity measurement value:

1. Generate a policy which has been agreed by each of the host and is aligned with key management services, and update into security policy database. The copy of policy is stored at secure storage

handled by Privacy CA. Each host has the same configuration value based on IPSec policy.

2. Generate a properties-based attestation as core integrity measurement based on the policy, and key management service ID and append with specific host ID such as MAC address and store it into the PCR. The PCR will encrypt this data at least with the specified TPM key or IPSec key.
3. Each host encrypts the core policy and then stores it at secure storage.

In our protocol, the initial remote attestation is performed using the IKE SA in phase 1 and attestation verification in phase 3. Figure 4 illustrates the detail process flow of the protocol. In phase 1, each communicating party needs to verify the desirable security policy, SAP1 with PCA to establish an initial IKE security association, SA1. As mentioned earlier the security policy become part of the IKE SA negotiation instead of nonce and DH key exchange. A data payload in this phase delivers the public part of AIK. Hence, after the parties validate the SAP with PCA, the SAP will be used as unique identifier to sign the AIK by the PCA. At the end of IKE's phase 1, each party have their respective AIK certificate verified by their respective TPM and established IKE security association, SA1. In phase 2, we use the standard IKEv2 protocol. Instead of using public key of each communicating party, the authentication message is signed using their AIK private key. The negotiated session key, SKAB and Child SAs, (SA2A, SA2B) is established in this phase and used to secure the message transmission subsequently. The attestation is performed in phase 3 to avoid eavesdropping since the IPSec channel has established. Each party computes the remote party's attestation nonce, *ncX=hash (NX|SKAB)* then prepare the TPM-quote containing ncx and second security policy, SAP2. Finally, each host verifies the remote's AIK certificate and computes TPM-quote using same nonce, SAP2 and compares it with the core integrity measurement.

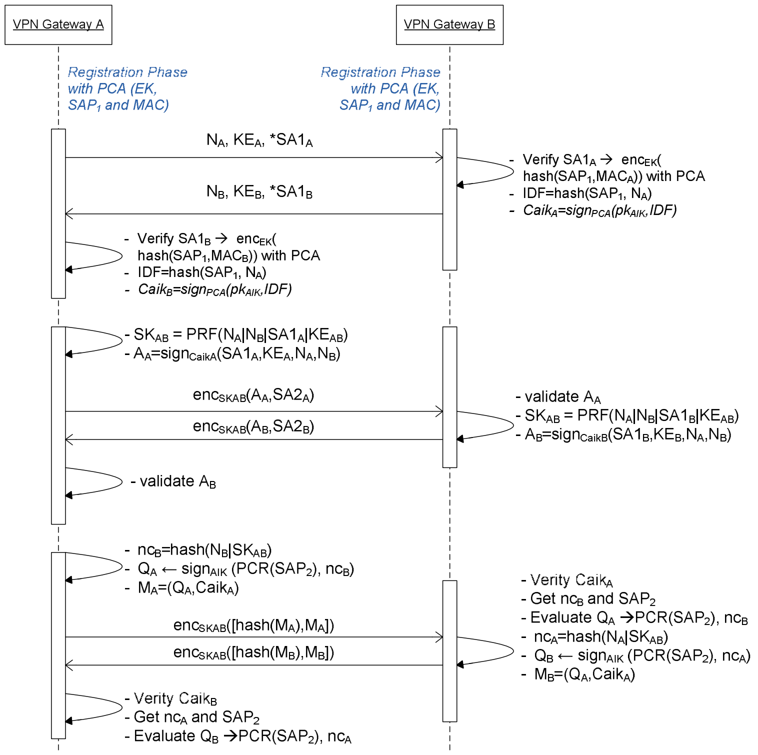
VPN Gateway A
VPN Gateway B
Registration Phase with PCA (EK, SAP_1 and MAC)
Registration Phase with PCA (EK, SAP_1 and MAC)
N_A, KE_A, $*SA1_A$
- Verify $SA1_A \rightarrow enc_{EK}($ $hash(SAP_1,MAC_A))$ with PCA
- $IDF=hash(SAP_1, N_A)$
- $Caik_A=sign_{PCA}(pk_{AIK},IDF)$
N_B, KE_B, $*SA1_B$
- Verify $SA1_B \rightarrow enc_{EK}($ $hash(SAP_1,MAC_B))$ with PCA
- $IDF=hash(SAP_1, N_A)$
- $Caik_B=sign_{PCA}(pk_{AIK},IDF)$
- $SK_{AB} = PRF(N_A|N_B|SA1_A|KE_{AB})$
- $A_A=sign_{CaikA}(SA1_A,KE_A,N_A,N_B)$
$enc_{SKAB}(A_A,SA2_A)$
$enc_{SKAB}(A_B,SA2_B)$
- validate A_A
- $SK_{AB} = PRF(N_A|N_B|SA1_B|KE_{AB})$
- $A_B=sign_{CaikB}(SA1_B,KE_B,N_A,N_B)$
- validate A_B
- $nc_B=hash(N_B|SK_{AB})$
- $Q_A \leftarrow sign_{AIK}(PCR(SAP_2), nc_B)$
- $M_A=(Q_A,Caik_A)$
$enc_{SKAB}([hash(M_A),M_A])$
$enc_{SKAB}([hash(M_B),M_B])$
- Verity $Caik_A$
- Get nc_B and SAP_2
- Evaluate $Q_A \rightarrow PCR(SAP_2)$, nc_B
- $nc_A=hash(N_A|SK_{AB})$
- $Q_B \leftarrow sign_{AIK}(PCR(SAP_2), nc_A)$
- $M_B=(Q_A,Caik_A)$
- Verity $Caik_B$
- Get nc_A and SAP_2
- Evaluate $Q_B \rightarrow PCR(SAP_2)$, nc_A

Figure 4: Integrating IKEv2 with Remote Attestation

As summary, the last step is IPSec establishment process consist of:

1. After attestation processes establish, A or B can send data to each other. Now, the IPSec communication using AIK certificate is embedding in ESP header and AH header.
2. Each time data arrives, A or B will verify the AIK certificate and the log.
3. The finger print of payload is signed with AIK key to generate signature as shown below:

$$\boxed{\text{sign(hash(payload), } \text{AIK}_{\text{key}})}$$

5. SECURITY CONSIDERATION

There are many security requirement for remote attestation solution has been discussed and identified in [11][18]. Most of them are focusing in security, privacy, authentic linkage of configuration information with secure channel and interoperability. We adopted some of the security requirement [11] as following:

- (SR1) Security: The integrity information must be cryptographically bound to the endpoints of the associated secure channel in order to prevent a compromised endpoint. It is to avoid relaying integrity report of other parties.
- (SR2) Privacy: Confidentiality of transmitted attestation message must be achieved comply with an organization's security policy.
- (SR3) Interoperability: The protocol extension must be well-suited with IKEv2.

Since our approach focus on IKEv2 secure channel and perform attestation after IKE SA2 is established, we achieve the security requirement SR1 and SR2. Through the attestation, the compromised platform will be detected because the integrity report is securely transferred through subsequent IPSec channel. This is based on assumptions that after the IKE phase 2 establishments, the channel is secure against replay attacks and packet loss because the transmit message is encrypted.

6. CONCLUSION

IPSec protocol provides a method for secure transmission of data and the authenticity of the communication. However, it does not assure the integrity of the involved endpoints platforms which can be solved by remote. We have proposed a protocol that utilizes the IKE negotiation of IPSec and attestation mechanism. The IKE management service is one of properties value in order to realize properties-based attestation mechanism in our extended IPSec. During the IKE negotiation, the remote attestation properties-based is established to measure the state of the end-to-end endpoint. Hence, through this protocol, besides protecting confidentiality, data integrity and origin authentication, it also guarantee the endpoint's integrity and privacy.

REFERENCES

[1] Trusted Computing Group. Retrieved from http://trustedcomputinggroup.org.

[2] TPM Main. 2005. Part 1 Design Principles. 1.2 revision 85 edition.

[3] Trusted Computing Group. 2008. TNC Architecture for Interoperability, v1.3.

[4] Trusted Computing Group. 2007. TNC TNC IF-IMC Specification, v1.2.

[5] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H. 2004. Extensible Authentication Protocol (EAP). RFC 3748, Updated by RFC 5247.

[6] Trusted Computing Group. 2007. TNC IF-T: Protocol Bindings for Tunneled EAP Methods, v1.1.

[7] Goldman, Kenneth and Perez, Ronald and Sailer, Reiner. 2006. Linking remote attestation to secure tunnel endpoints. *Proceedings of the first ACM workshop on Scalable trusted computing,* ISBN: 1-59593-548-7, ACM. RFC23982.

[8] Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn. 2004. Attestation-based Policy Enforcement for Remote Access, *Proceedings of the 11th ACM conference on Computer and communications security*, ISBN: 1-58113-961-6, ACM.

[9] Haidong Xia, Jayashree Kanchana and Jose' Carlos Brustoloni. 2006. *Enforcement of Security Policy Compliance in Virtual Private Network*, University of Pittsburgh, USA.

[10] Ahmad-Reza Sadeghi, Steffen Schulz. 2009. Secure VPNs for trusted computing environments. *Proceeding Trust '09 Proceedings of the 2nd International Conference on Trusted Computing*, LNCS, vol. 5471, pp. 197–216. Springer, Heidelberg.

[11] Ahmad-Reza Sadeghi, Steffen Schulz. 2010. Extending IPSec for Efficient Remote Attestation. *Proceeding, FC'10 Proceedings of the 14th international conference on Financial cryptography and data security*, ISBN:3-642-14991-X 978-3-642-14.

[12] Ingo Bente, Bastian Hellmann, Joerg Vieweg, Josef von Helden, and Arne Welzel. 2011. *Interoperable Remote Attestation in VPN Environments*, In: Chen, L., Mitchell, C.J., Martin, A. (eds.) INTRUST 2010. LNCS, vol. 6802, pp. 302–315. Springer, Heidelberg.

[13] Kaufman, C. 2010. Internet Key Exchange (IKEv2) Protocol. RFC 5996.

[14] Natarajan Meghanathan. *A Tutorial on Network Security: Attacks and Controls*. Jackson State University.

[15] Sebastian Modersheim, Paul Hankes Drielsma. 2003. IKEv2-DS, AVISPA Project, Retrieved from http://www.avispa-project.org/library/ IKEv2-DS.html.

[16] Norazah, A. A., Lucyantie, M. 2009. Identity Credential Issuance with Trusted Computing. *2nd International Conference on Computing and Informatics, ICOCI '09*.

[17] Ahmad-Reza Sadeghi and Christian Stuble. 2004. Property-based attestation for computing platforms: caring about properties, not mechanisms, *Proceedings of the 2004 workshop on New security paradigms*, ISBN:1-59593-076-0, ACM.

[18] F. Armknecht, Y., Gasmi, Sadeghi, A., Stewin, P., Unger, M. 2008. An efficient implementation of trusted channels based on OpenSSL. *Proc. of 3rd ACM workshop on Scalable Trusted Computing*, pp. 41-50, ACM Press.