International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.119-134
http://dx.doi.org/10.14257/ijsia.2016.10.10.12

Security Analysis and Improvement of the TNC IF-T Protocol Binding for Tunneled EAP Methods

Yuelei Xiao[1,2,3]

[1]*Institute of IOT and IT-based Industrialization, Xi'an University of Posts and Telecommunications, Xi'an 710061, China*
[2]*Shaanxi Provincial Information Engineering Research Institute, Xi'an 710075, China*
[3]*School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China*
xiao_yuelei@163.com

Abstract

The TNC IF-T Protocol Binding for Tunneled EAP Methods (TIPBTEM) is specified by Trusted Computing Group (TCG) for TNC assessment (i.e., Platform-Authentication) exchanges. Because the TIPBTEM includes Platform-Authentication in addition to the usual user authentication, it differs greatly from the traditional security protocols in terms of security requirements. To analyze the security of the TIPBTEM correctly, the extended strand space model (SSM) for trusted network access protocols is applied in this paper. And it is pointed out that the TIPBTEM cannot prevent man-in-the-middle (MITM) attacks in some cases. To eliminate MITM attacks, the unsecure cases of the TIPBTEM are improved based on cryptographic binding. And then it is showed that these improved TIPBTEM cases can resist MITM attacks in the extended SSM.

Keywords*: Platform-Authentication, strand space model, man-in-the-middle attacks*

1. Introduction

With the rapid development of network technologies, network security problems (including viruses, spywares, trojan horses, *etc*.) are getting more and more serious. Traditional network security systems are composed of firewalls, intrusion detection systems, antivirus systems, *etc*. However, they cannot stand up to the growing network security problems because of the two reasons as follows: (1) defending themselves from external attacks other than internal attacks; (2) ignoring the protection of endpoints, which are places for creating and storing important data, and initiate most attacks [1]. To solve this problem, trusted network access technologies were proposed in the industry, mainly including TCG's Trusted Network Connect (TNC), Cisco's Network Admission Control (NAC) and Microsoft's Network Access Protection (NAP) [2, 3]. Although they have similar aims and technologies, they have different emphases for their own backgrounds. Hence, the interoperability among them was established to make it easier for users to choose [4, 5]. Additionally, Huawei Technologies co., ltd had put forward an Endpoint Admission Defense (EAD) solution [6], and TOPSEC co., ltd had proposed a Trusted Network Architecture (TNA) [7].

The TNC architecture defined by TCG [2] is one of the most typical trusted network access technologies. In the TNC architecture, Platform-Authentication is crucial for the security and authorization of network-access requests in addition to the usual user authentication [2]. And Platform-Authentication pertains to two related aspects of authentication. The first aspect is the proof of identity of the platform (or platform

ISSN: 1738-9976 IJSIA

credential authentication), while the second aspect is the integrity verification (or integrity check handshake) of the platform. One important part of the TNC architecture is IF-T, which is a standard protocol used to transport the TNC assessment (*i.e.*, Platform-Authentication) exchanges leveraging the existing network connectivity. Because the TNC assessment exchanges occur when the endpoint is in the process of joining the network or after the endpoint has been placed on the network, several bindings of the IF-T exist to address these different scenarios, *e.g.*, the TNC IF-T Protocol Binding to TLS (TIPBT) and the TIPBTEM [8, 9]. The TIPBT focuses on the IF-T usage model where the endpoint is already present on the network, while the TIPBTEM focuses on the IF-T usage model where the endpoint is in the process of joining the network.

In the TIPBT and TIPBTEM, Platform-Authentication is performed in addition to the usual user authentication. Therefore, they differ greatly from the traditional security protocols in terms of security requirements. Although the strand space model (SSM) [10-12] is a well-studied formal method for security protocols, it cannot be used to analyze the security of them directly due to the above reason. To overcome this problem, an extended SSM for trusted network access protocols was proposed and used to analyze the security of the TIPBT [13, 14]. One important part of the extended SSM is that the external penetrator (keys set $\mathcal{K}_{ep}$) and the internal penetrator (keys set $\mathcal{K}_{ip}$) are introduced, and the theorem for Platform-Authentication is given. In this paper, the extended SSM is also used to analyze the security of the TIPBTEM. The analysis results indicate that the TIPBTEM cannot prevent MITM attacks in some instances. To resist MITM attacks, the TIPBTEM is improved based on cryptographic binding. And then it is showed that the improved TIPBTEM can successfully prevent MITM attacks in the extended SSM.

The rest of this paper is organized as follows. Section 2 gives an overview of the TIPBTEM. In Section 3, the extended SSM is used to analyze the security of the TIPBTEM. And it is pointed out that the TIPBTEM cannot prevent MITM attacks in some instances. In Section 4, the TIPBTEM is improved based on cryptographic binding. And it is proved that the improved TIPBTEM can successfully prevent MITM attacks in the extended SSM. Finally, the conclusion is presented in Section 5.

2. Overview of the TIPBTEM

The TIPBTEM mainly includes two distinct phases [9]: (1) tunnel establishment; (2) running an EAP-TNC method (*i.e.*, a special EAP method for encapsulating and exchanging TNC assessment messages) and other EAP methods (realizing client side authentication) over the tunnel created in the first phase. The TIPBTEM is illustrated in Figure 1.

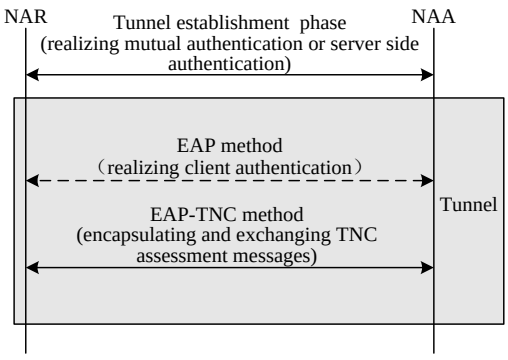

Figure 1. The process of the TIPBTEM

In Figure 1, an outer tunneled EAP method is performed to realize mutual or server side authentication during the tunnel establishment phase, where the outer tunneled EAP method could be initiated by either the Network Access Requestor (NAR) or the Network Access Authority (NAA). In the TCG's TNC architecture, the NAR is a component of the Access Requestor (AR), while the NAA is a component of the Policy Decision Point (PDP). When mutual authentication is implemented during the first phase, only the EAP-TNC method is performed over the tunnel created in the first phase. However, when server side authentication is implemented during the first phase, other EAP methods need to be performed over the tunnel created in the first phase to realize client side authentication before the EAP-TNC method is performed over the tunnel created in the first phase. Moreover, to prevent MITM attacks, a Diffie-Hellman Pre-Negotiation (D-H PN) protocol may be added in the EAP-TNC method, then the inner key established by the D-H PN protocol and the outer key established by the outer tunneled EAP method are mixed to protect the following data communication. The detail process of the TIPBTEM with the D-H PN protocol is illustrated in Figure 2.

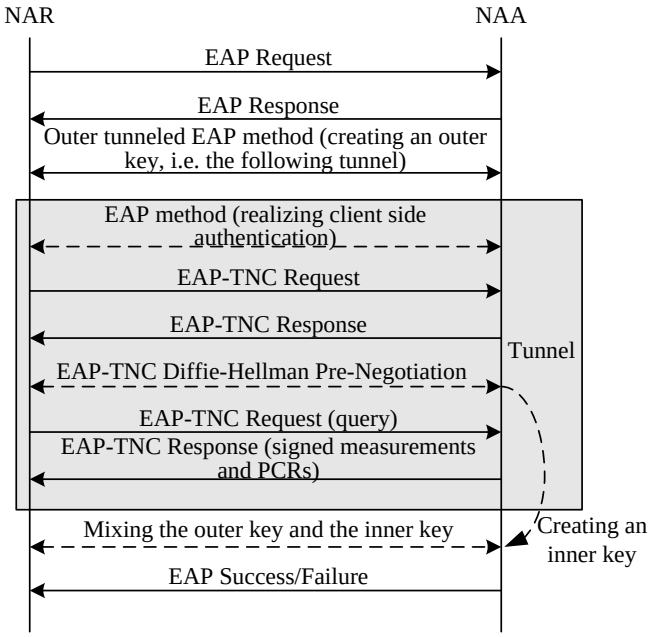

Figure 2. The Detailed Process of the TIPBTEM with the D-H PN Protocol

In Figure 2, after the EAP-TNC method completes, an additional tunneled EAP method round trip is required to mix the outer key and the inner key, and assure that both the NAR and the NAA have computed the same mixed key. The process of the D-H PN protocol is as follows:

(1) NAR ← NAA: D-H PN Hello Request
(2) NAR → NAA: D-H PN Hello Response
(3) NAR ← NAA: D-H PN Parameters Request
(4) NAR → NAA: D-H PN Parameters Response

where D-H PN Hello Request and D-H PN Hello Response are used to negotiate some parameters for Diffie-Hellman (DH) exchange, and D-H PN Parameters Request and D-H PN Parameters Response are used for DH exchange. D-H PN Parameters Request includes g^z and N_{PDP}, while D-H PN Parameters Response includes g^t and

N_{AR}, where g^t is a temporal public key for DH exchange generated by the AR, g^z is a temporal public key for DH exchange generated by the PDP, N_{AR} is a random number of the AR, N_{PDP} is a random number of the PDP. After the NAR receives D-H PN Parameters Request, it computes $Unique-Value-1=H(1\|N_{AR}\|N_{PDP}\|g^{zt})$ and $Unique-Value-2=H(2\|N_{AR}\|N_{PDP}\|g^{zt})$, where g^{zt} is a D-H PN secret key and $H()$ is a hash function. And the NAA also computes $Unique-Value-1=H(1\|N_{AR}\|N_{PDP}\|g^{zt})$ and $Unique-Value-2=H(2\|N_{AR}\|N_{PDP}\|g^{zt})$ after it receives D-H PN Parameters Response. Both the NAR and the NAA must compute a running hash $Unique-Value-2=H(Unique-Value-2\|H(EAP-TNC\ message))$ when the D-H PN protocol has successfully completed. This running hash is performed repeatedly after receiving or sending an EAP-TNC message. The final $Unique-Value-2$ is a value which is cryptographically computed from the D-H PN secret key, nonce pair and all of the EAP-TNC Responses, *i.e.*, the inner key.

3. Security Analysis of the TIPBTEM

To simplify the security analysis of the TIPBTEM, we give some assumptions as follows.

- The outer tunneled EAP method is based on the TLS protocol [15]. This means that the outer key is created by the TLS handshake protocol. The TLS handshake protocol is initiated by the NAR. And the simplified version of the TLS handshake protocol [12] is considered in this paper. When mutual authentication between the NAR and the NAA is implemented by the TLS handshake protocol during the tunnel establishment phase, a traditional client side X.509 certificate or a client side X.509 certificate including the Subject Key Attestation Evidence (SKAE) extension [16] is used to authenticate the client, *i.e.*, the AR.
- If the authentication of the client has not occurred during the tunnel establishment phase, then it will be implemented by exchanging Client Authentication Messages with the Basic Authentication type of authentication [8].
- In the EAP-TNC protocol, only one round trip of TNC assessment messages is exchanged, which is simplified to the integrity challenge protocol in [17].
- The mixing and assuring of the outer key and the inner key is based on the three pass authentication mechanism in [18].

According to these assumptions, the TIPBTEM can be summarized into five cases as follows, where the notations are the same as those in [10-12, 17].

Case a): only server authentication is implemented during the tunnel establishment phase, and the D-H PN protocol is not performed in the EAP-TNC method. The process of this case is as follows:

(1) NAR → NAA: AR

(2) NAR ← NAA: $PDP\|g^x\|\sigma_{PDP}$

(3) NAR → NAA: $g^y\|MAC_{AR}$

(4) NAR ← NAA: MAC_{PDP}

(5) NAR ← NAA: $\{chall_{client-auth}\}_{K^o_{AR,PDP}}$

(6) NAR → NAA: $\{resp_{client-auth}\}_{K^o_{AR,PDP}}$

(7) NAR ← NAA: $\{N_{PDP,2}\}_{K^o_{AR,PDP}}$

(8) NAR → NAA: $\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}$

where AR and PDP identify the AR and the PDP in the TCG's TNC architecture respectively, σ_{PDP} is a signature of the PDP and $\sigma_{PDP} = [g^x]_{sk_{PDP}}$, sk_{PDP} is a private key of the PDP, MAC_{AR} is a message authentication code of the AR and $MAC_{AR} = H_{K^o_{AR,PDP}}(T_1 \| AR \| PDP)$, MAC_{PDP} is a message authentication code of the PDP and $MAC_{AR} = H_{K^o_{AR,PDP}}(T_1 \| AR \| PDP)$, $H_K()$ is a message authentication code function, $K^o_{AR,PDP}$ is the outer key created by the TLS handshake protocol and $K^o_{AR,PDP} = H(g^{xy})$, T_1 and T_2 are fixed tags to distinguish the third message from the fourth message, $chall_{client-auth}$ and $resp_{client-auth}$ are a Client Authentication Challenge Message and a Client Authentication Response Message for the client side authentication based on the selected authentication type respectively, $resp_{client-auth} = AR \| PW_{AR}$ and PW_{AR} is a password of the AR that is registered at the PDP prior to initiating the TIPBTEM, α is the platform of the AR, PCR_α is a Platform Configuration Register (PCR) list of α, SML_α is a Stored Measurement Log (SML) of α, $Cert(AIK_{pub,\alpha})$ is an Attestation Identity Key (AIK) certificate, $AIK_{pub,\alpha}$ is an AIK public key of α, σ_α is a signature of α and $\sigma_\alpha = [N_{PDP,2} \| PCR_\alpha]_{AIK_{priv,\alpha}}$, $AIK_{priv,\alpha}$ is an AIK private key of α.

Case b): mutual authentication based on a traditional client side X.509 certificate is implemented during the tunnel establishment phase, and the D-H PN protocol is not performed in the EAP-TNC method. The process of this case is as follows:

(1) NAR → NAA: AR
(2) NAR ← NAA: $PDP \| g^x \| \sigma_{PDP}$
(3) NAR → NAA: $g^y \| \sigma_{AR} \| MAC_{AR}$
(4) NAR ← NAA: MAC_{PDP}
(5) NAR ← NAA: $\{N_{PDP,2}\}_{K^o_{AR,PDP}}$
(6) NAR → NAA: $\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}$

where σ_{AR} is a signature of the AR and $\sigma_{AR} = [g^y]_{sk_{AR}}$, sk_{AR} is a private key of the AR.

Case c): mutual authentication based on a client side X.509 certificate including the SKAE extension is implemented during the tunnel establishment phase, and the D-H PN protocol is not performed in the EAP-TNC method. The process of this case is the same as that of case b) except that a client side X.509 certificate including the SKAE extension is used in the tunnel establishment phase.

Case d): only server authentication is implemented during the tunnel establishment phase, and the D-H PN protocol is performed in the EAP-TNC method. The process of this case is as follows:

(1) NAR → NAA: AR
(2) NAR ← NAA: $PDP \| g^x \| \sigma_{PDP}$
(3) NAR → NAA: $g^y \| MAC_{AR}$
(4) NAR ← NAA: MAC_{PDP}
(5) NAR ← NAA: $\{chall_{client-auth}\}_{K^o_{AR,PDP}}$

(6) NAR → NAA: $\{resp_{client-auth}\}_{K^o_{AR,PDP}}$

(7) NAR ← NAA: $\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(8) NAR → NAA: $\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(9) NAR ← NAA: $\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(10) NAR → NAA: $\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(11) NAR ← NAA: $\{N_{PDP,2}\}_{K^o_{AR,PDP}}$

(12) NAR → NAA: $\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}$

(13) NAR ← NAA: $N_{PDP,3}$

(14) NAR → NAA: $N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}$

(15) NAR ← NAA: $N_{AR,3} \| MAC_{PDP,2}$

where $reqHello_{D-H\ PN}$ and $respHello_{D-H\ PN}$ are D-H PN Hello Request and D-H PN Hello Response in the EAP-TNC method respectively, $reqParams_{D-H\ PN} = g^y \| N_{PDP,2}$ and $respParams_{D-H\ PN} = g^x \| N_{AR,2}$ are D-H PN Parameters Request and D-H PN Parameters Response in the EAP-TNC method respectively, σ_α is changed to $\sigma_\alpha = [H(N_{PDP,2} \| Unique-Value-1) \| PCR_\alpha]_{AIK_{priv,\alpha}}$, $N_{AR,3}$ is another random number of the AR, $N_{PDP,3}$ is another random number of the PDP, $MAC_{AR,2}$ is another message authentication code of the AR and $MAC_{AR,2} = H_{K^m_{AR,PDP}}(N_{PDP,3} \| N_{AR,3})$, $MAC_{PDP,2}$ is another message authentication code of the PDP and $MAC_{PDP,2} = H_{K^m_{AR,PDP}}(N_{AR,3})$, $K^m_{AR,PDP} = H(K^o_{AR,PDP} \| K^i_{AR,PDP})$ is a mixed key from $K^o_{AR,PDP}$ and $K^i_{AR,PDP}$, $K^i_{AR,PDP}$ is the inner key created by the D-H PN protocol and $K^i_{AR,PDP}$ is the final $Unique-Value-1$.

Case e): mutual authentication based on a traditional client side X.509 certificate is implemented during the tunnel establishment phase, and the D-H PN protocol is performed in the EAP-TNC method. The process of this case is as follows:

(1) NAR → NAA: AR

(2) NAR ← NAA: $PDP \| g^x \| \sigma_{PDP}$

(3) NAR → NAA: $g^y \| \sigma_{AR} \| MAC_{AR}$

(4) NAR ← NAA: MAC_{PDP}

(5) NAR ← NAA: $\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(6) NAR → NAA: $\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}$;

(7) NAR ← NAA: $\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(8) NAR → NAA: $\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}$

(9) NAR ← NAA: $\{N_{PDP,2}\}_{K^o_{AR,PDP}}$

(10) NAR → NAA: $\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}$

(11) NAR ← NAA: $N_{PDP,3}$

(12) NAR → NAA: $N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}$

(13) NAR ← NAA: $N_{AR,3} \| MAC_{PDP,2}$

where σ_α is changed to $\sigma_\alpha = [H(N_{PDP,2} \| Unique-Value-1) \| PCR_\alpha]_{AIK_{priv,\alpha}}$.

3.1. Security Analysis of Case a) of the TIPBTEM

Definition 1: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for case a) of the TIPBTEM if Σ is the union of three kinds of strands:

(1) Penetrator strands $s \in \mathcal{P}$.

(2) Initiator strands $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$ with trace: $<+AR, -PDP \| g^x \| \sigma_{PDP}, +g^y \| MAC_{AR}, -MAC_{PDP}, -\{chall_{client-auth}\}_{K^o_{AR,PDP}}, +\{resp_{client-auth}\}_{K^o_{AR,PDP}}, -\{N_{PDP,2}\}_{K^o_{AR,PDP}}, +\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}>$. The principal associated with this strand is $AR \cdot \alpha$ (*i.e.*, the AR), which is a two-identity protocol participant [13]. AR denotes the user of the AR, α denotes the platform of the AR.

(3) Responder strands $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$ with trace: $<-AR, +PDP \| g^x \| \sigma_{PDP}, -g^y \| MAC_{AR}, +MAC_{PDP}, +\{chall_{client-auth}\}_{K^o_{AR,PDP}}, -\{resp_{client-auth}\}_{K^o_{AR,PDP}}, +\{N_{PDP,2}\}_{K^o_{AR,PDP}}, -\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}>$. The principal associated with this strand is PDP (*i.e.*, the PDP).

Theorem 1: Suppose: (1) $\sum$ is a space for case a) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

Proof. By assumption (2), $\sigma_{PDP} = [g^x]_{sk_{PDP}} \subset term(<s,2>)$ never originates on an external penetrator strand. If $sk_{PDP} \notin \mathcal{K}_{ip}$, then $[g^x]_{sk_{PDP}}$ must originate on a responder strand r, and g^x uniquely arises on r by Definition 1 and assumption (3). By assumption (1) and (3), g^y uniquely arises on s. Since the protocol of Definition 1 is both silent and conservative, g^{xy} never originates in C (Theorem 9 in [12]). Since $K^o_{AR,PDP} = H(g^{xy}) \notin \mathcal{K}_p$, $term(s,4)$, $term(s,5)$ and $term(s,7)$ originate on r by assumption (3). Similarly, $term(r,3)$, $term(r,6)$ and $term(r,8)$ originate on s by assumption (3). By inspection, $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

If $sk_{PDP} \in \mathcal{K}_{ip}$, then PDP as an internal penetrator can complete the entire exchange, which is identical to that PDP as a regular completes the entire exchange. Hence, PDP as an internal penetrator cannot perform effective attacks on case a) of the TIPBTEM.

Theorem 2: Suppose: (1) $\sum$ is a space for case a) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$; (2) $PW_{AR} \notin \mathcal{K}_{ep}$; (3) SML_α

indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha'$, PDP', $(g^x)'$, $(g^y)'$, $(chall_{client-auth})'$, $resp_{client-auth}$, $(N_{PDP,2})'$, $(PCR_\alpha)'$, $(SML_\alpha)'$, $(Cert(AIK_{pub,\alpha}))']$ and an initiator strand $r' \in \text{Init}[AR'' \cdot \alpha$, PDP'', $(g^x)''$, $(g^y)''$, $(chall_{client-auth})''$, $(resp_{client-auth})''$, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})]$.

Proof. By assumption (2), $resp_{client-auth} \subset term(s,6)$ never originates on an external penetrator strand. If $PW_{AR} \notin \mathcal{K}_{ip}$, then $resp_{client-auth}$ must originate on an initiator strand $r \in \text{Init}[AR \cdot \alpha'$, PDP', $(g^x)'$, $(g^y)'$, $(chall_{client-auth})'$, $resp_{client-auth}$, $(N_{PDP,2})'$, $(PCR_\alpha)'$, $(SML_\alpha)'$, $(Cert(AIK_{pub,\alpha}))']$. Additionally, by assumption (3), $\sigma_\alpha \subset term(s,8)$ must originate on an initiator strand $r' \in \text{Init}[AR'' \cdot \alpha$, PDP'', $(g^x)''$, $(g^y)''$, $(chall_{client-auth})''$, $(resp_{client-auth})''$, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})]$ (Theorem 1 in [13]).

If $PW_{AR} \in \mathcal{K}_{ip}$, we can only get that $\sigma_\alpha \subset term(s,8)$ must originate on the initiator strand r' by assumption (3) (Theorem 1 in [13]).

According to Theorem 1, C contains a responder strand that is the same as that of Definition 1, *i.e.*, the initiator's guarantee of agreement is proved. Thus, $AR \cdot \alpha$ authenticates PDP successfully. In Theorem 2, if $PW_{AR} \notin \mathcal{K}_{ip}$, then C contains an initiator strand that is deferent from that of Definition 1, *i.e.*, the responder's guarantee of agreement is not proved. Hence, we can know that an external penetrator can perform MITM attacks on this case of the TIPBTEM, similar to [19]. Moreover, if $PW_{AR} \in \mathcal{K}_{ip}$, then C also contains an initiator strand that is deferent from that of Definition 1, *i.e.*, the responder's guarantee of agreement is also not proved. Therefore, this case of the TIPBTEM cannot prevent an internal penetrator performing a MITM attack similar to the collaborative masquerading attack described in [20].

3.2. Security Analysis of Case b) of the TIPBTEM

Definition 2: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for case b) of the TIPBTEM if Σ is the union of three kinds of strands:

(1) Penetrator strands $s \in \mathcal{P}$.

(2) Initiator strands $s \in \text{Init}[AR \cdot \alpha$, PDP, g^x, g^y, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})]$ with trace: $<+AR$, $-PDP \| g^x \| \sigma_{PDP}$, $+g^y \| \sigma_{AR} \| MAC_{AR}$, $-MAC_{PDP}$, $-\{N_{PDP,2}\}_{K^o_{AR,PDP}}$, $+\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}>$. The principal associated with this strand is $AR \cdot \alpha$.

(3) Responder strands $s \in \text{Resp}[AR \cdot \alpha$, PDP, g^x, g^y, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})]$ with trace: $<-AR$, $+PDP \| g^x \| \sigma_{PDP}$, $-g^y \| \sigma_{AR} \| MAC_{AR}$, $+MAC_{PDP}$, $+\{N_{PDP,2}\}_{K^o_{AR,PDP}}$, $-\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}>$. The principal associated with this strand is PDP.

Theorem 3: Suppose: (1) Σ is a space for case b) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha$, PDP, g^x, g^y, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in Σ,

and $g^x \neq g^y$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

Proof: It is similar to Theorem 1.

Theorem 4: Suppose: (1) Σ is a space for case b) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$; (2) $sk_{AR} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$; (4) SML_α indicates that the legitimate platform α is trustworthy. If $sk_{AR} \notin \mathcal{K}_{ip}$, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$, otherwise C contains an initiator strand $r' \in \text{Init}[AR' \cdot \alpha, PDP', (g^x)', (g^y)', N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

Proof: By assumption (2), $\sigma_{AR} = [g^y]_{sk_{AR}} \subset term(s,3)$ never originates on an external penetrator strand. If $sk_{AR} \notin \mathcal{K}_{ip}$, then σ_{AR} must originate on an initiator strand r, and g^y uniquely arises on r by Definition 2 and assumption (3). By assumption (1) and (3), g^x uniquely arises on s. Since the protocol of Definition 2 is both silent and conservative, g^{xy} never originates in C. Since $K^o_{AR,PDP} = H(g^{xy}) \notin \mathcal{K}_p$, $term(s,3)$ and $term(s,6)$ originate on r by assumption (3). Similarly, $term(r,4)$ and $term(r,5)$ originate on s. By inspection, $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

If $sk_{AR} \in \mathcal{K}_{ip}$, we can only get that $\sigma_\alpha \subset term(s,6)$ must originate on the initiator strand $r' \in \text{Init}[AR' \cdot \alpha, PDP', (g^x)', (g^y)', N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$ by assumption (4) (Theorem 1 in [13]).

According to Theorem 3, C contains a responder strand that is the same as that of Definition 2, *i.e.*, the initiator's guarantee of agreement is proved. And by Theorem 4, C contains an initiator strand that is the same as that of Definition 2 if $sk_{AR} \notin \mathcal{K}_{ip}$ (*i.e.*, the responder's guarantee of agreement is proved). Thus, in comparison with case a) of the TIPBTEM, this case of the TIPBTEM can prevent MITM attacks performed by the external penetrator. However, if $sk_{AR} \in \mathcal{K}_{ip}$, then C also contains an initiator strand that is deferent from that of Definition 2, i.e., the responder's guarantee of agreement is also not proved. Therefore, it still cannot prevent an internal penetrator performing the same MITM attack as the collaborative masquerading attack described in [20].

3.3. Security Analysis of Case c) of the TIPBTEM

Definition 3: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for case c) of the TIPBTEM if Σ is the union of the same three kinds of strands as those of Definition 2. The only significant difference is that AR's certificate is an X.509 certificate including the SKAE extension.

Theorem 5: Suppose: (1) Σ is a space for case c) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in $\sum$,

and $g^x \neq g^y$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

Proof: It is similar to Theorem 1.

Theorem 6: Suppose: (1) Σ is a space for case c) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$; 2 g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$; (3) SML_α indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

Proof: Because sk_{AR} is a non-migratable or Certified Migratable Key (CMK) signing key, and created in the TPM of α [17], $\sigma_{AR} = [g^y]_{sk_{AR}} \subset term(s,3)$ never originates on a penetrator strand by assumption (3) (Theorem 1 in [13]). Therefore, σ_{AR} must originate on an initiator strand r, and g^y uniquely arises on r by Definition 3 and assumption (2). By assumption (1) and (2), g^x uniquely arises on s. Since the protocol of Definition 3 is both silent and conservative, g^{xy} never originates in C. Since $K^o_{AR,PDP} = H(g^{xy}) \notin \mathcal{K}_p$, $term(s,3)$ and $term(s,6)$ originate on r by assumption (3). Similarly, $term(r,4)$ and $term(r,5)$ originate on s. By inspection, $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha})]$.

According to Theorem 5, C contains a responder strand that is the same as that of Definition 3, *i.e.*, the initiator's guarantee of agreement is proved. And by Theorem 6, C contains an initiator strand that is the same as that of Definition 3, *i.e.*, the responder's guarantee of agreement is proved. Therefore, this case of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator.

3.4. Security Analysis of Case d) of the TIPBTEM

Definition 4: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for case d) of the TIPBTEM if Σ is the union of three kinds of strands:

(1) Penetrator strands $s \in \mathcal{P}$.

(2) Initiator strands $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$ with trace: $\langle +AR, -PDP \| g^x \| \sigma_{PDP}, +g^y \| MAC_{AR}, -MAC_{PDP}, -\{chall_{client-auth}\}_{K^o_{AR,PDP}}, +\{resp_{client-auth}\}_{K^o_{AR,PDP}}, -\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{N_{PDP,2}\}_{K^o_{AR,PDP}}, +\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}, -N_{PDP,3}, +N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}, -N_{AR,3} \| MAC_{PDP,2} \rangle$. The principal associated with this strand is $AR \cdot \alpha$.

(3) Responder strands $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$ with trace: $<-AR, +PDP \| g^x \| \sigma_{PDP}, -g^y \| MAC_{AR}, +MAC_{PDP}, +\{chall_{client-auth}\}_{K^o_{AR,PDP}}, -\{resp_{client-auth}\}_{K^o_{AR,PDP}}, +\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{N_{PDP,2}\}_{K^o_{AR,PDP}}, -\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}, +N_{PDP,3}, -N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}, +N_{AR,3} \| MAC_{PDP,2} >$. The principal associated with this strand is PDP.

Theorem 7: Suppose: (1) $\sum$ is a space for case d) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x, g^y, g^z and g^t are uniquely arising in $\sum$, and $g^x \neq g^y \neq g^z \neq g^t$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$.

Proof: It is similar to Theorem 1.

Theorem 8: Suppose: (1) $\sum$ is a space for case d) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$; (2) g^x, g^y, g^z and g^t are uniquely arising in $\sum$, and $g^x \neq g^y \neq g^z \neq g^t$; (3) SML_α indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$.

Proof: By assumption (3), $\sigma_\alpha \subset term(s,12)$ must originate on an initiator strand r (Theorem 1 in [13]), and g^t uniquely arises on r by Definition 4 and assumption (2). By assumption (1) and (2), g^z uniquely arises on s. Since the protocol of Definition 4 is both silent and conservative, g^{zt} never originates in C. Because $Unique-Value-2 = H(2 \| N_{AR} \| N_{PDP} \| g^{zt})$, $Unique-Value-2 = H(Unique-Value-2 \| H(EAP-TNC\ message))$ and the final $Unique-Value-2$ is $K^i_{AR,PDP}$, $K^i_{AR,PDP} \notin \mathcal{K}_p$. Since $K^m_{AR,PDP} = H(K^o_{AR,PDP} \| K^i_{AR,PDP}) \notin \mathcal{K}_p$, $MAC_{AR,2} \subset term(s,14)$ originate on an

initiator strand r', and g^y uniquely arises on r' by Definition 4 and assumption (2). By assumption (1) and (2), g^x uniquely arises on s. Since the protocol of Definition 4 is both silent and conservative, g^{xy} never originates in C. Since $K^o_{AR,PDP} = H(g^{xy}) \notin \mathcal{K}_p$, $term(s,3)$, $term(s,6)$, $term(s,8)$, $term(s,10)$, $term(s,12)$ and $term(s,14)$ originate on $r = r'$ by assumption (2). Similarly, $term(r,4)$, $term(r,5)$, $term(r,7)$, $term(r,9)$, $term(r,11)$, $term(r,13)$ and $term(r,15)$ originate on s by assumption (2). By inspection, $r = r' \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$.

According to Theorem 7, C contains a responder strand that is the same as that of Definition 4, *i.e.*, the initiator's guarantee of agreement is proved. And from Theorem 8, C contains an initiator strand that is the same as that of Definition 4, *i.e.*, the responder's guarantee of agreement is proved. Therefore, this case of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator.

3.5. Security Analysis of Case e) of the TIPBTEM

Definition 5: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for case e) of the TIPBTEM if Σ is the union of three kinds of strands:

(1) Penetrator strands $s \in \mathcal{P}$.

(2) Initiator strands $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$ with trace: $\langle +AR, -PDP \| g^x \| \sigma_{PDP}, +g^y \| \sigma_{AR} \| MAC_{AR}, -MAC_{PDP}, -\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{N_{PDP,2}\}_{K^o_{AR,PDP}}, +\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}, -N_{PDP,3}, +N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}, -N_{AR,3} \| MAC_{PDP,2} \rangle$. The principal associated with this strand is $AR \cdot \alpha$.

(3) Responder strands $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$ with trace: $\langle -AR, +PDP \| g^x \| \sigma_{PDP}, -g^y \| \sigma_{AR} \| MAC_{AR}, +MAC_{PDP}, +\{reqHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{respHello_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{reqParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, -\{respParams_{D-H\ PN}\}_{K^o_{AR,PDP}}, +\{N_{PDP,2}\}_{K^o_{AR,PDP}}, -\{PCR_\alpha \| SML_\alpha \| Cert(AIK_{pub,\alpha}) \| \sigma_\alpha\}_{K^o_{AR,PDP}}, +N_{PDP,3}, -N_{PDP,3} \| N_{AR,3} \| MAC_{AR,2}, +N_{AR,3} \| MAC_{PDP,2} \rangle$. The principal associated with this strand is PDP.

Theorem 9: Suppose: (1) $\sum$ is a space for case e) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth},$

$resp_{client-auth}$, $reqHello_{D-H\ PN}$, $respHello_{D-H\ PN}$, $reqParams_{D-H\ PN}$, $respParams_{D-H\ PN}$, $N_{PDP,2}$, PCR_α, SML_α, $Cert(AIK_{pub,\alpha})$, $N_{AR,3}$, $N_{PDP,3}]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x, g^y, g^z and g^t are uniquely arising in $\sum$, and $g^x \neq g^y \neq g^z \neq g^t$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$.

Proof: It is similar to Theorem 1.

Theorem 10: Suppose: (1) $\sum$ is a space for case e) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha, PDP, g^x, g^y, chall_{client-auth}, resp_{client-auth}, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$; (2) g^x, g^y, g^z and g^t are uniquely arising in $\sum$, and $g^x \neq g^y \neq g^z \neq g^t$; (3) SML_α indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y, reqHello_{D-H\ PN}, respHello_{D-H\ PN}, reqParams_{D-H\ PN}, respParams_{D-H\ PN}, N_{PDP,2}, PCR_\alpha, SML_\alpha, Cert(AIK_{pub,\alpha}), N_{AR,3}, N_{PDP,3}]$.

Proof: It is similar to Theorem 8.

According to Theorem 9, C contains a responder strand that is the same as that of Definition 5, *i.e.*, the initiator's guarantee of agreement is proved. And by Theorem 10, C contains an initiator strand that is the same as that of Definition 5, *i.e.*, the responder's guarantee of agreement is proved. Therefore, this case of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator.

4. Improvement of the TIPBTEM

To overcome the MITM attacks on both case a) and b) of the TIPBTEM, it is necessary to bind the Platform-Authentication and usual user authentication of the AR. If $K^o_{AR,PDP}$ is generated on α, then $K^o_{AR,PDP}$ cannot be migrated because α is trustworthy. $K^o_{AR,PDP}$ is used to protect the usual user authentication of the AR in case a) of the TIPBTEM, and directly generated during the usual user authentication of the AR in case b) of the TIPBTEM, so the Platform-Authentication and usual user authentication of the AR are bound. Hence, we only need to change $\sigma_\alpha = [N_{PDP,2} \| PCR_\alpha]_{AIK_{priv,\alpha}}$ to $\sigma_\alpha = [H(N_{PDP,2} \| K^o_{AR,PDP}) \| PCR_\alpha]_{AIK_{priv,\alpha}}$, *i.e.*, cryptographically bind $K^o_{AR,PDP}$ to σ_α, making that $K^o_{AR,PDP}$ is generated on σ_α. Then, it is proved that the improved case a) and b) of the TIPBTEM can prevent MITM attacks performed by both the external penetrator and the internal penetrator.

Definition 6: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for the improved case a) of the TIPBTEM if Σ is the union of the same three kinds of strands as those of Definition 1. The only significant difference is $\sigma_\alpha = [H(N_{PDP,2} \| K^o_{AR,PDP}) \| PCR_\alpha]_{AIK_{priv,\alpha}}$.

Theorem 11: Suppose: (1) $\sum$ is a space for the improved case a) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha, PDP, g^x, g^y,$

$chall_{client-auth}$, $resp_{client-auth}$, $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha$, PDP , g^x , g^y , $chall_{client-auth}$, $resp_{client-auth}$, $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$.

Proof: It is the same as Theorem 1.

Theorem 12: Suppose: (1) $\sum$ is a space for the improved case a) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha$, PDP , g^x , g^y , $chall_{client-auth}$, $resp_{client-auth}$, $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$; (2) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$; (3) SML_α indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha$, PDP , g^x , g^y , $chall_{client-auth}$, $resp_{client-auth}$, $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$.

Proof: By assumption (3), $\sigma_\alpha \subset term(s,8)$ must originate on an initiator strand r , and g^y uniquely arises on r by Definition 6 and assumption (2). By assumption (1) and (2), g^x uniquely arises on s . Since the protocol of Definition 6 is both silent and conservative, g^{xy} never originates in C . Since $K^o_{AR,PDP} = H(g^{xy}) \notin \mathcal{K}_p$, $term(s,3)$, $term(s,6)$ and $term(s,8)$ originate on r by assumption (2). Similarly, $term(r,4)$, $term(r,5)$ and $term(r,7)$ originate on s . By inspection, $r \in \text{Init}[AR \cdot \alpha$, PDP , g^x , g^y , $chall_{client-auth}$, $resp_{client-auth}$, $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$.

According to Theorem 11, C contains a responder strand that is the same as that of Definition 6, *i.e.*, the initiator's guarantee of agreement is proved. And by Theorem 12, C contains an initiator strand that is the same as that of Definition 6, *i.e.*, the responder's guarantee of agreement is proved. Therefore, the improved case a) of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator.

Definition 7: An infiltrated strand space $\Sigma, \mathcal{P}$ is a space for the improved case b) of the TIPBTEM if Σ is the union of the same three kinds of strands as those of Definition 2. The only significant difference is $\sigma_\alpha = [H(N_{PDP,2} \| K^o_{AR,PDP}) \| PCR_\alpha]_{AIK_{priv,\alpha}}$.

Theorem 13: Suppose: (1) Σ is a space for the improved case b) of the TIPBTEM, and C is a bundle containing an initiator strand $s \in \text{Init}[AR \cdot \alpha$, PDP , g^x , g^y , $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$; (2) $sk_{PDP} \notin \mathcal{K}_{ep}$; (3) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$. Then, C contains a responder strand $r \in \text{Resp}[AR \cdot \alpha$, PDP , g^x , g^y , $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$.

Proof: It is the same as Theorem 1.

Theorem 14: Suppose: (1) Σ is a space for case b) of the TIPBTEM, and C is a bundle containing a responder strand $s \in \text{Resp}[AR \cdot \alpha$, PDP , g^x , g^y , $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$; (2) g^x and g^y are uniquely arising in $\sum$, and $g^x \neq g^y$; (3) SML_α indicates that the legitimate platform α is trustworthy. Then, C contains an initiator strand $r \in \text{Init}[AR \cdot \alpha$, PDP , g^x , g^y , $N_{PDP,2}$, PCR_α , SML_α , $Cert(AIK_{pub,\alpha})]$.

Proof: It is similar to Theorem 12.

According to Theorem 13, C contains a responder strand that is the same as that of Definition 7, *i.e.*, the initiator's guarantee of agreement is proved. And by Theorem 14, C contains an initiator strand that is the same as that of Definition 7, *i.e.*, the responder's guarantee of agreement is proved. Therefore, this improved case b) of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator.

5. Conclusions

The TCG's TNC architecture is one of the most typical trusted network access technologies. And one important part of the TCG's TNC architecture is IF-T, including several bindings of the IF-T exist to address these different scenarios, *e.g.*, the TIPBT and the TIPBTEM. Because the TIPBTEM includes Platform-Authentication in addition to the usual user authentication, it differs greatly from the traditional security protocols in terms of security requirements. In order to analyze the security of the TIPBTEM correctly, the extended SSM for trusted network access protocols is applied in this paper. Firstly, five cases are illustrated according to the overview of TIPBTEM. And some assumptions are given to simplify the security analysis of the TIPBTEM. Secondly, security analysis of the TIPBTEM is performed based on this extended SSM. And the analysis results indicate that case a) of the TIPBTEM cannot prevent MITM attacks performed by both the external penetrator and the internal penetrator, case b) of the TIPBTEM can prevent MITM attacks performed by the external penetrator while it cannot prevent MITM attacks performed by the internal penetrator, and case c), d) and e) of the TIPBTEM can prevent MITM attacks performed by both the external penetrator and the internal penetrator. In order to eliminate these MITM attacks, both case a) and b) of the TIPBTEM are improved based on cryptographic binding. Finally, it is proved that the improved case a) and b) of the TIPBTEM can successfully prevent MITM attacks performed by both the external penetrator and the internal penetrator in the extended SSM.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61402367).

References

[1] C. Shen, "Build up protection system of active defense and comprehensive on-guard", China Information Security, vol. 41, no. 5, **(2004)**, pp. 17-18.
[2] Trusted Computing Group, "TNC Architecture for Interoperability Specification", Available online: http://www.trustedcomputinggroup.org/tnc-architecture-interoperability-specification, **(2016)**.
[3] U.D.Q Hasham, "Comparative study of network access control technologies", Master Dissertation, Linköping University, **(2007)**.
[4] H. Zhang, L. Chen and L. Zhang, "Research on trusted network connection", Chinese Journal of Computers, vol. 33, no. 4, **(2010)**, pp. 706-717.
[5] Q. Feng, Z. Wang, X. Li and W. Zhou, "Trusted network connect technology based on 802.1X", Computer Engineering, vol. 35, no. 5, **(2009)**, pp. 165-167.
[6] H3C, "EAD solution", Available online: http://www.h3c.com.cn/Solution/Mobility/EAD, **(2016)**.
[7] TOPSEC, "TNA 2.0", Available online: http://www.topsec.com.cn/jjfa/aqln/jsjg/index.htm, **(2016)**.
[8] Trusted Computing Group, "TNC IF-T: Binding to TLS Specification", Available online: http://www.trustedcomputinggroup.org/tnc-if-t-binding-tls, **(2016)**.
[9] Trusted Computing Group, "TNC IF-T: Protocol Bindings for Tunneled EAP Methods Specification", Available online: http://www.trustedcomputinggroup.org/tnc-if-t-protocol-bindings-tunneled-eap-methods-specification, **(2016)**.

[10] F.J.T. Fábrega, J.C. Herzog and J.D. Guttman, "Strand spaces: why is security protocol correct?", Proceedings of the 1998 IEEE Symposium on Security and Privacy, Oakland, CA, USA, **(1998)** May 3-6.
[11] F.J.T. Fábrega, J.C. Herzog and J.D. Guttman, "Strand space: proving security protocols correct", Journal of Computer Security, vol. 7, no. 2-3 **(1999)**, pp. 191-230.
[12] J.C. Herzog, "The Diffie-Hellman key-agreement scheme in the strand-space model", Proceedings of the 16th IEEE Computer Security Foundation Workshop, Pacific Grove, California, USA, **(2003)** June 30-July 2.
[13] Y. Xiao, Y. Wang and L. Pang, "Verification of trusted network access protocols in the strand space model", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E95-A, no. 3, **(2012)**, pp. 665-668.
[14] Y. Xiao, Y. Wang and L. Pang, "Security Analysis and Improvement of TNC IF-T Protocol Binding to TLS", China Communications, vol. 10, no. 7, **(2013)**, pp. 85-92.
[15] RFC, "The Transport Layer Security (TLS) Protocol Version 1.2", Available online: http://www.ietf.org/rfc/rfc5246.txt, **(2016)**.
[16] Trusted Computing Group, "Infrastructure Work Group Subject Key Attestation Evidence Extension, Version 1.0", Available online: http://www.trustedcomputinggroup.org/infrastructure-work-group-subject-key-attestation-evidence\linebreak-extension-version-1-0, **(2016)**.
[17] R. Sailer, X. Zhang, T. Jaeger and L.V. Doom, "Design and implementation of a TCG-based integrity measurement architecture", Proceedings of the 13th USENIX Security Symposium, Lake Tahoe, California, USA, **(2004)** August 9-13.
[18] ISO/IEC 9798-4:1999, "Information Technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function", Available online: http://www.iso.org/iso, **(2016)**.
[19] N. Asokan, V. Niemi and K. Nyberg, "Man-in-the-Middle in tunneled authentication protocols", Proceedings of the 11th International Workshop on Security Protocols, Cambridge,UK, **(2003)** April 2-4.
[20] F. Stumpf, O. Tafreschi and P. Roder, "A robust integrity reporting protocol for remote attestation", Proceedings of the 2nd Workshop on Advances in Trusted Computing, Ivy Hall Aogaku Kaikan, Tokyo, Japan, **(2006)** November 30-December 1.

Author

Yuelei Xiao, he graduated from Xidian University in Telecommunication Engineering, and his master's degree in Xi'an Jiao Tong University. Now he is mainly engaged in the research of security protocols analysis and trusted computing.

