LETTER

Trusted Inter-Domain Fast Authentication Protocol in Split Mechanism Network

Lijuan ZHENG[†,††a)], Yingxin HU[††], Zhen HAN[†], *Nonmembers*, *and* Fei MA[†], *Student Member*

SUMMARY Previous inter-domain fast authentication schemes only realize the authentication of user identity. We propose a trusted inter-domain fast authentication scheme based on the split mechanism network. The proposed scheme can realize proof of identity and integrity verification of the platform as well as proof of the user identity. In our scheme, when the mobile terminal moves to a new domain, the visited domain directly authenticates the mobile terminal using the ticket issued by the home domain rather than authenticating it through its home domain. We demonstrate that the proposed scheme is highly effective and more secure than contemporary inter-domain fast authentication schemes.

key words: *split mechanism, trusted computing, inter-domain fast authentication*

1. Introduction

In traditional networks, the IP address is not only used to denote identity information of the host but also its location information, which leads to the route scalability problem. So it is difficult for the Internet to support mobility and multi-homing [1]. Internet Architecture Board (IAB) solves the IP address semantics overload problem by introducing two namespaces to represent the identifier and location of a node, that is “Locator/Identifier Split” [2].

In this paper, the Internet is divided into a core network and multiple access networks. Access IDentifier (AID) and Routing IDentifier (RID) are introduced. AID represents public identity information of Mobile Node (MN), which includes identifier of MN, type of MN etc. When MN moves in the network, AID remains unchanged. RID represents location information of MN and is used for routing. RID includes the identifier of a domain, subnet identifier of Access Switch Router (ASR) and so on. When MN moves, ASR will assign a new RID to it. The communication between the user and access network is accomplished through the use of AID. Transmission of packets in the core network is accomplished through the use of RID. A link between AID and RID is established by building an access identity resolution map. This resolution map is implemented by ASR [3].

In a split mechanism network, when the mobile terminal moves to a different domain, it needs to be reauthenticated. If we select the method of access authentication, terminals that handoff frequently will experience unacceptable latency, which is fatal for some real-time services. Therefore, an inter-domain fast authentication method should be designed to minimize the handover process.

Many inter-domain fast authentication methods have been proposed, which includes [4]–[7]. Through research analysis we can discover that the existing fast authentication methods only realize the authentication of the terminal user identity. They do not consider platform identity and platform credibility of the terminal. Unfortunately, most current information security threats come from within the network. It is urgent to prevent terminal platforms from acting maliciously, i.e. virus insertion and tampering. Trusted computing technology proposed by Trusted Computing Group (TCG) can solve this problem effectively. Trusted computing guarantees the existing terminal security through binding a Trusted Platform Module (TPM) on the terminal [8].

TPM is a separate trusted coprocessor. TPM has a set of Platform Configuration Registers (PCRs) [9], which are used to store platform integrity measurement values. When TPM measures a component, it creates an event and records it in Stored Measurement Log (SML). PCR value and SML value are used together to prove the status of the platform. In order to guarantee that the PCR value is credible, TPM uses the Attestation Identity Key (AIK) private key to sign the PCR value. The verifier uses AIK public key to verify the signature value of PCR, and judges whether the platform is credible by comparing SML to the PCR value.

We first construct a trusted inter-domain fast authentication model framework. Then we propose a trusted inter-domain fast authentication protocol. The proposed scheme can realize proof of identity and integrity verification of the platform as well as the proof of user identity. Through security and performance analysis, we show that our protocol is more secure and has better performance.

The remainder of this paper is organized as follows: Sect. 2 gives the trusted inter-domain fast authentication model framework. Section 3 describes the trusted inter-domain fast authentication protocol in detail. In Sect. 4, we analyze the security and performance, and conclusion is discussed in Sect. 5.

Manuscript received April 23, 2012.

Manuscript revised July 4, 2012.

[†] The authors are with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China.

[††] The authors are with the School of Information Science and Technology, Shijiazhuang Tiedao University, Hebei Province, China.

a) E-mail: 07112083@bjtu.edu.cn

DOI: 10.1587/transinf.E95.D.2728

Copyright © 2012 The Institute of Electronics, Information and Communication Engineers

2. Trusted Inter-Domain Fast Authentication Model Framework

Trusted inter-domain fast authentication model framework is displayed in Fig. 1.

MN is a wireless terminal. A TPM chip is embedded in it. AC$_H$ (Authentication Center in MN's home domain) is responsible for the register of the terminal, proof of user identity and generation of the ticket. Privacy-CA$_H$ (Privacy-Certificate Authority in MN's home domain) is responsible for the verification of MN and issue AIK public key certificate. GAC (Global Authentication Center) is a global authentication server, which assigns key to each AC used to signing ticket. In the Home Domain (HD), MN connects to the network through ASR. When MN first accesses, AC$_H$ and Privacy-CA$_H$ together authenticate identity and integrity of the platform, which ensures validity of the identity and credibility of the platform. Suppose that MN has already completed the registration in its hometown domain, and passed proof of user identity and platform. AIK public key certificate and SML are stored in a secure manner by AC$_H$. When MN roams to a different domain, it sends the ticket issued by AC$_H$ to AC$_F$. Then AC$_F$ decrypts the ticket and verifies the identity and platform of the MN.

3. Protocol Description

3.1 Symbol Explanation

Symbols used in the protocol are defined in Table 1.

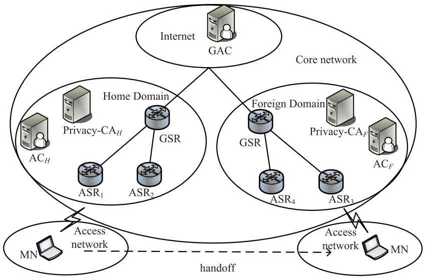

Fig. 1 Trusted inter-domain fast authentication model framework.

Table 1 Symbol definition.

Symbol	Definition
ID_A	identifier of entity A
AID_A	access identifier of entity A
K_{A-B}	key shared between entity A and B
K_{ticket}	the key used to issue ticket
$E_K(M)$	symmetric encryption with key K to message M
$(M)_K$	signature with key K to message M
AIK_A^{Pub}	AIK public key of platform A
AIK_A^{Priv}	AIK private key of platform A
$Cert(AIK_A^{Pub})$	AIK public key certificate of platform A
T_A	time stamp generated by entity A
R_A	a random number generated by entity A

3.2 Generation of the Ticket

GAC shares K_{ticket} with all ACs. Each AC uses K_{ticket} to generate the Ticket for local registered user. The generation of the $Ticket_{MN}$ can be expressed in Eq. (1).

$$\begin{aligned} Ticket_{MN} = E_{K_{ticket}}(&AID_{MN}, SML, Cert(AIK_{MN}^{Pub}) \\ &K_{MN}, Lifetime_{MN}, ID_{AC_H}) \end{aligned} \quad (1)$$

AID_{MN} is the access identifier of MN; K_{MN} is the key owned by MN, which is known by AC_H and stored in it; $Lifetime_{MN}$ is the expiry date of the certificate of MN issued by AC_H, and it also represents the expiry date of the ticket; ID_{AC_H} is the identifier of AC_H. SML is a measurement stored log of MN. $Cert(AIK_{MN}^{Pub})$ is AIK public key of MN platform. When MN's access authentication is complete, it submits SML and $Cert(AIK_{MN}^{Pub})$ to AC_H.

3.3 Trusted Inter-Domain Fast Authentication Protocol

When MN completes access authentication in HD, AC_H encrypts $Ticket_{MN}$ using K_{MN} and sends it to MN. MN saves $Ticket_{MN}$.

The protocol is displayed in Fig. 2.

Suppose MN roams from ASR_1 to ASR_3, the authentication process in detail is as follows:

1) When MN roams to ASR_3, it extracts $Ticket_{MN}$ and $(PCR)_{AIK_{MN}^{Priv}}$, then sends the message $Ticket_{MN}$, $E_{K_{MN}}((PCR)_{AIK_{MN}^{Priv}}, AID_{MN}, T_{MN})$ to ASR_3.

2) After ASR_3 receives this message from MN, it forwards it directly to AC_F.

3) AC_F uses K_{ticket} to decrypt $Ticket_{MN}$ and gets $(AID_{MN}, SML, Cert(AIK_{MN}^{Pub}), K_{MN}, Lifetime_{MN}, ID_{AC_H})$.

AC_F first verifies the validity of $Lifetime_{MN}$. If $Lifetime_{MN}$ is invalid, authentication fails. If $Lifetime_{MN}$ is valid, AC_F uses K_{MN} to decrypt $E_{K_{MN}}((PCR)_{AIK_{MN}^{Priv}}, AID_{MN}, T_{MN})$, and gets $(PCR)_{AIK_{MN}^{Priv}}$, AID_{MN} and T_{MN}.

Then AC_F compares whether this AID_{MN} is the same as AID_{MN} in $Ticket_{MN}$. If they are the same, it shows that MN's identification is credible, otherwise authentication fails.

At last, AC_F verifies the platform.

AC_F uses $Cert(AIK_{MN}^{Pub})$ to verify $(PCR)_{AIK_{MN}^{Priv}}$ and compares PCR value in SML to current PCR value. If they are equal, then verify the identity of the MN platform and platform integrity. Hence, authentication to MN completes.

4) AC_F precomputes PMK_0. PMK_0 is a random number decided by AC_F. AC_F assigns master key PMK_0 used

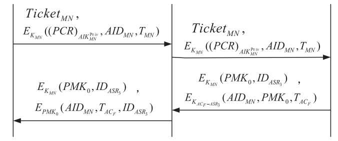
MN
ASR_3
AC_F
$Ticket_{MN}$,
$E_{K_{MN}}((PCR)_{AIK_{MN}^{Priv}}, AID_{MN}, T_{MN})$
$Ticket_{MN}$,
$E_{K_{MN}}((PCR)_{AIK_{MN}^{Priv}}, AID_{MN}, T_{MN})$
$E_{K_{MN}}(PMK_0, ID_{ASR_3})$,
$E_{K_{AC_F-ASR_3}}(AID_{MN}, PMK_0, T_{AC_F})$
$E_{K_{MN}}(PMK_0, ID_{ASR_3})$,
$E_{PMK_0}(AID_{MN}, T_{AC_F}, ID_{ASR_3})$

Fig. 2 Trusted inter-domain fast authentication protocol.

by MN and ASR_3 to MN, and sends the authentication result $E_{K_{AC_F-ASR_3}}(AID_{MN}, PMK_0, T_{AC_F})$, $E_{K_{MN}}(PMK_0, ID_{ASR_3})$ to ASR_3. $K_{AC_F-ASR_3}$ is the key shared by AC_F and ASR_3.

5) ASR_3 receives authentication success message, updates its mapping table, admits MN to access, and sends $E_{PMK_0}(AID_{MN}, T_{AC_F}, ID_{ASR_3})$, $E_{K_{MN}}(PMK_0, ID_{ASR_3})$ to MN. In the following process, MN and ASR_3 will use PMK_0 to negotiate session keys. If authentication fails, it will return MN "authentication failure" information.

4. Security and Performance Analysis

4.1 Security Analysis

1) security of $Ticket$

Secret information $Ticket_{MN}$ is encrypted by K_{ticket} which is shared by AC_H and AC_F. This key is issued by GAC and used by ACs in each domain to issue ticket. It is confidential to other members, which ensures the security and unforgeability of $Ticket_{MN}$.

2) anti-replay

T_{MN} is embedded in the message encrypted by K_{MN}. Even if someone intercepts $E_{K_{MN}}((PCR)_{AIK^{Priv}_{MN}}, AID_{MN}, T_{MN})$ and replays it. AC_F can detect it according to the T_{MN}. AC_F extracts time stamp T_{MN} in $E_{K_{MN}}((PCR)_{AIK^{Priv}_{MN}}, AID_{MN}, T_{MN})$, and compares it to its current time. If the time interval is less than five minutes, AC_F agrees that the information is authentic. Otherwise the information is considered too old, outdated, and the requester is not trusted.

For duplicate message received within five minutes, even if the time-stamp is not old, will be discarded. Since this message may be a replayed message. We can store the messages within five minutes. If the messages are stored for longer than five minutes, they will be deleted. So when a new message is coming, we can compare it to the stored messages, if they are the same, we will not process it.

So the protocol can resist replay attack.

3) anonymity of user identification

MN's real identity is not appeared in the messages during the protocol interaction process. We use MN's access identification AID_{MN} to represent MN. Only its local authentication center AC_H has some of the MN's private information. AC_H is securely protected, so MN's private information can not flow outside, thus ensuring the anonymity of user identification.

4) location privacy of mobile node

MN's correspond node only knows MN's AID. MN's RID is hidden inside the network, so it can not obtain. For the eavesdroppers, in the access network they can see only the mobile node's AID, and cannot trace mobile node's RID. In the core network, they can only obtain the mobile node's RID, but was unable to reverse track the mobile node's AID. An eavesdropper cannot obtain corresponding relationship between identity and topological location information of mobile node. Therefore, the mobile node's location privacy is well protected.

Table 2 Protocol security comparison.

Security Metric	ours	CPK-F	IWAA	SSP	SEP
user anonymity	Y	N	Y	Y	N
mutual authentication	Y	Y	Y	Y	Y
anti-replay	Y	Y	Y	Y	Y
key negotiation fairness	Y	N	N	Y	Y
proof of platform identity	Y	Y	N	N	N
platform integrity verification	Y	Y	N	N	N

Table 3 Protocol performance comparison.

Performance Metric	ours	CPK-F	IWAA	SSP	SEP
hash operation times	1	1	1	2	2
exponential operation times	0	0	2	3	0
symmetric encryption times	4	0	2	4	7
symmetric decryption times	4	0	1	3	7
public key encryption times	1	3	0	0	0
public key decryption times	0	3	0	0	0

5) Platform identity credibility and platform integrity

PCR sent to AC_F by MN is signed using AIK private key. When AC_F verifies, it use AIK public key in $Ticket_{MN}$ to decrypt. MN's AIK private key is only owned by MN platform, and others have no way to get. Thus the identity of MN platform is verified.

After AC_F gets PCR, it compares it to SML in $Ticket_{MN}$. If they are equal, platform integrity of MN can be guaranteed.

We compare our protocol with CPK-F in [4], IWAA in [5], SSP (Protocol based on Self-Certified) in [6], SEP (Protocol based on Self-Encryption) in [7] in security and performance. Please look at Table 2 to get the security comparing results.

4.2 Performance Analysis

The efficiency of the protocol is measured by the calculations performed in the protocol, including exponentiation operation, hash operation, symmetric encryption/decryption, public key encryption/ decryption and so on.

Performance analysis and comparison of results are shown in Table 3.

During the authentication process, the CPU and TPM in the mobile terminal can do some encryption/decryption operation in parallel, which shortens the computation time and reduces the communication delay. A public key encryption process and a symmetric key encryption are done by the TPM, and the terminal does not consume the CPU computing performance. The execution speed of symmetric encryption is much faster than public key encryption/decryption and exponentiation operation.

The protocol interaction will not generate a great flow on the network. It just needs a message passed back and forth, reducing the network traffic. Fast authentication process does not require the AC in its home domain, reducing the burden of the home domain AC, and also shortening the authentication delay.

On the whole, the proposed inter-domain fast authentication protocol has a higher efficiency and better security.

5. Conclusion

In this paper, we proposed a trusted inter-domain fast authentication scheme for split mechanism networks. Compared with other fast authentication schemes, our scheme is more secure and more effective. It can realize the dual authentication of terminal and platform, anonymity and untraceability of user identification, anonymity and anti-replay of platform. It can realize fast authentication in a foreign domain using the ticket issued by the AC in its home domain while not requiring direct involvement of the home AC. It reduces the burden of the AC in its home domain and also shortens the authentication delay. The ticket proposed in this paper is not valid forever but has a term of validity. This involves life time setting and regeneration of the ticket, which is also the question that we must consider as a next step.

Acknowledgement

This work is supported by the "863" program of China under Grant No.2007AA01Z410 and 2007AA01Z177, the Program of Changjiang Scholars and Innovative Research Team in University, the program of Ministry of Education Innovative Research Team under Grant No.IRT0707, National Natural Science Funds of K09A300150, Hebei Natural Science Funds of F2009000927, Hebei Educational Committee Foundation of Z2011160.

References

[1] D. Clark, R. Braden, A. Falk, and V. Pingali, "FARA: Reorganizing the addressing architecture," Proc. ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA), pp.313–321, Karlsruhe, Germany, Aug. 2003.

[2] H. Balakrishnan, K. Lakshminarayanan, S. Ramasamy, S. Shenker, I. Stoica, and M. Walfish, "A layered naming architecture for the Internet," ACM SIGCOMM Computer Communication Review, vol.34, no.4, pp.343–352, Aug. 2004.

[3] D. Ping, Y. Dong, Y.J. Qin, and H.K. Zhang, "Research on the mobility management scheme in future Internet," Acta Electronica Sinica, vol.36, no.10, pp.1916–1922, Oct. 2008.

[4] J. Zhang, Y.J. Zhang, H.W. Zhang, and Z.C. Li, "A fast inter-domain authentication method combining trust mechanism in mobile ipv6 networks," J. Computer Research and Development, vol.45, no.6, pp.951–959, June 2008.

[5] H.X. Peng and D.G. Feng, "Security flaws and improvement to a wireless authentication protocol with anonymity," J. Communications, vol.27, no.9, pp.78–85, Sept. 2006.

[6] Y.X. Jiang, C. Lin, X.M. (Sherman) Shen, and M.H. Hui, "Mutal authentication and key exchange protocols for roaming services in wireless mobile networks," IEEE Trans. Wireless Commun., vol.5, no.9, pp.2569–2577, Sept. 2006.

[7] K.F. Hwang and C.C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans. Wireless Commun., vol.2, no.2, pp.400–407, March 2003.

[8] Trusted Computing Group, "TCG specification architecture overview," http://www.trusted computing group.org, accessed Aug. 3. 2011.

[9] M.J. Zhang, W.M. Gui, and D.S. Su, "Trusted computing technique from terminal to network," Information Technology Bulletin, vol.4, no.2, pp.21–31, March 2006.