Jurnal Teknologi

Full paper

Security and Privacy Criteria to Evaluate Authentication Mechanisms in Proxy Mobile IPv6

Mojtaba Alizadeh[a*], Mazdak Zamani[b], Sabariah Baharun[a], Wan Haslina Hassan[a], Touraj Khodadadi[a]

[a]*Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia*
[b]*Advanced Informatics School, Universiti Teknologi Malaysia, Federal Territory, 54100 Kuala Lumpur, Malaysia*

*Corresponding author: amojtaba2@live.utm.my

Article history

Received : 15 August 2014
Received in revised form :
15 October 2014
Accepted :15 November 2014

Abstract

Mobility management protocols support mobility for roaming mobile nodes in order to provide seamless connectivity. Proxy Mobile IPv6 is a network-based localized mobility management protocol that is more suitable for resource constrained devices among different mobility management schemes. In this protocol, all mobility signaling procedures are completed by network entity not mobile node. According to the Proxy Mobile IPv6 architecture, an authentication procedure has a key role to protect the network against different security threats; however, the details of authentication procedure is not specified in this standard. In this paper, different security features are explored to evaluate the authentication protocols in Proxy Mobile IPv6. The existing authentication approaches can be analyzed based on these criteria to find security issues.

Keywords: Authentication; security and privacy; proxy Mobile IPv6; PMIPv6

■1.0 INTRODUCTION

Todays, enormous growth can be seen in the wireless and mobile devices as most people employ mobile devices to access various services such as multimedia applications, video conferencing, file sharing, and browsing the internet at anytime, anywhere [1]. Although, mobile devices are facing various problems to use wireless services that include some problems such as low computing power of mobile terminals, insufficient channel capacity and complex security problems. The Mobile IPv6 (MIPv6) [2] is an Internet Engineering Task Force standard, which adds the capabilities of the roaming of mobile nodes in IPv6 network. This standard permits mobile devices to travel between networks by keeping mobile nodes connected to the network. Even though, Mobile IPv6 is mostly aimed for mobile devices, it is utilized for wired environments [3]. The Mobile IPv6 requirement is essential as the mobile nodes in a fixed IPv6 network cannot preserve the connected link while location is changed.

The Mobile IPv6 protocol suffers from several problems such as packet loss, delay, and signaling cost. Therefore, different host-based mobility management protocols like hierarchical Mobile IPv6 (HMIPv6) [4], fast handover for Mobile IPv6 (FMIPv6) [5] and network-based mobility management protocols like Proxy Mobile IPv6 (PMIPv6) [6], are proposed to improve performance of MIPv6. In comparison hierarchical Mobile IPv6 protocol with fast handover for Mobile IPv6 (FMIPv6), the Proxy Mobile IPv6 (PMIPv6) achieves high less handover latency and signaling cost [7].

The Network-based Localized Mobility Management (NETLMN) working group of IETF [8] standardized Proxy Mobile IPv6 (PMIPv6) [6], which is a network-based mobility management protocol. In PMIPv6, the mobility services are provided without mobile node (MN) involvement in signaling communications. This protocol that decreases mobility signaling over wireless links, is chosen as a part of different wireless network such as WiMAX, 3GPP2, as well as LAN networks [9].

The main mobility entities are the Local Mobility Anchor (LMA) along with the Mobile Access Gateway (MAG) in PMIPv6 domain. The LMA supports MN connectivity and the MAG, running typically on the access router, accomplishes mobility management instead of the MN. Consequently, an MN with in PMIPv6 does not need modification of the protocol stack to support PMIPv6. All mobility signaling is managed by the MAG and LMA establishing bi-directional tunnel to conduct the traffic sent to/from the MN. In the MN view, the entire domain of PMIPv6 seems as its home network [7].

■2.0 SECURITY SERVICES IN PROXY MOBILE IPV6

2.1 Authentication

The authentication process is the verifying device's identity or a user's process for the communication purpose [10]. In Proxy Mobile IPv6, MN must be authenticated to the network mutually in the first place. Whenever the MN connects to a network, it wants to be confident to not be recognized as a malicious network. At the same time, the network requires to make sure that the MN is the one he/she claims to be and that MN is eligible to have an access to the service. On the other hand, the present specification prepares no authentication scheme [9].

2.2 Location verification

Considering the attack of Malicious Mobile Node Flooding (MMF), it is not sufficient to authenticate just MNs and BU messages. To overcome this kind of attack, it is required to find that if MNs certainly exist in their claimed CoA and HoA [11].

■3.0 SECURITY AND PRIVACY CRITERIA

3.1 User Anonymity

One of the significant properties of entities is their privacy that a protocol should preserve it, and avoid other adversaries from masquerading legal users [12-14]. In networks of MIPv6, if the CoA and the home address of MN are transferred as plaintext in the binding update messages, thus any eavesdropper can reveal them. Identifying the mobile node, home address, as well as the present location, care of address, can result in a major damage to the privacy of the mobile nodes. However, the trade-off between the privacy and anonymity on one side and performance on other side makes proposing suitable method to preserve anonymity more difficult [15].

3.2 Mutual Authentication

In order to preserve the legitimate party security and avoid adversaries from impersonating and compromising, an authentication protocol planned should prepare mutual authentication for server and user to promise that all authenticated entities are safe in an unsecure environment [16]. The MN must be mutually authenticated with the MAG in the step of communication procedure. The mobility service and the authorizations for the network access services are transparently provided to the mobile node [17].

3.3 Session Key Secrecy

After successful authentication procedure, transferring data between user and server is required. Thus, an authentication protocol must contain essential exchange phase in order to meet this requirement [18]. The Session Key Secrecy includes two parts, namely Backward and Forward Secrecy. The forward secrecy guarantees that the passive adversary may not have the ability to derive succeeding session keys without knowing about key subset. On the other hand, the Backward Secrecy ensures that an inactive adversary may not have the capability to acquire the preceding session keys without having information about key subset [19].

3.4 User Unlinkability

A user unlinkability simply defined as authentic messages that cannot be linked and identified to particular user [20]. Unlinkability guarantees that users can employ services or resources without others ability to link the employment of services together. Unlinkability attributes eliminates any probable linkage between two successive IP handovers accomplished by a similar mobile node in hiding the mobile node's current location [21].

■4.0 ATTACKS ON PROXY MOBILE IPV6

4.1 Session Hijacking (SSH)

The main goal of SSH attack is to steal victims' session and to redirect data traffic by masquerading victims. In this attack, at the first step, the MN1 is a victim that wants to communicate the CN. The binding update is forged by an attacker to claim that the MN1 has moved to new domain in the networks. At that point, the new Care of Address (CoA) is assigned to MN1 that is CoA of MN2, the attacker. In successful case, the attack redirect the traffic of MN1 to MN2 and the information leakage is happened [11].

4.2 Malicious Mobile Node Flooding (MMF)

The goal of MMF attack is to make victims flooded with several packets or to redirect network traffic to the malicious MNs [22]. Before initiating this attack, the attacker must communicate with some CNs and send its CNs a binding update message indicating that it has moved to the victim node's place. If the CNs confirm the message, the MN's traffic is redirected to the victim Node simultaneously [11].

4.3 Verifier Impersonation

A form of active eavesdropping is the impersonation attack that the attacker creates independent connection with the victims and sends messages between them, causing them to think that they can directly talk to each other over a private connection while indeed the whole conversation is directed by the attacker [23].

4.4 Replay Attack

Replay attack contains the passive capture of data and its subsequent retransmission to create an unauthorized effect. A malicious node preserves an authentication message in order to create a false report of normal node and then it may transfer previous authentication message in order to deceive the AAA/Policy server for wrong authentication [24].

4.5 Man-in-the-middle Attack

Another attack during the gaining access stage is the Man in the Middle, or well known as MITM, that the attacker locates himself/herself in the middle of the communication of data between two parties. An attacker uses this attack to launch further attacks, including session hijacking and sniffing. In Proxy Mobile IPv6, an attacker that handles to interject between the legitimate MAG and MN may sniff the data traffic as well as control communication signaling. If the attacker is on the original data plane path, he can drop, modify and forge route update packets in order to make wrong route establishment or the routes removal [25].

4.6 Insider Attack

It is launched by an entity inside the security perimeter, that is to say, an entity authorized to access system resources though it employs them in a manner not accepted by those granted the authorization. The insider attack may result in important security holes in an authentication protocol. In this situations, a local administrator (LMA) acquires the mobile node password, and she/he attempts to imitate the user to access MAG [26].

4.7 Modification Attack

An adversary may try to change the authentication message of the MAG or the MN. In order to protect the Proxy Mobile IPv6 network against this kind of attack, some solution should be proposed to make sure that information cannot be changed. Thus, the attack will be identified if an attacker cannot acquire the nonce value to create the legitimate message. If the attacker transfers a malicious (modified) packet to the authentication server or the MN, the packet should be recognized easily by checking its values [27].

4.8 Eavesdropping

Eavesdropping is kind of stealing information attack and it can be active or passive. A passive eavesdropping attack occurs while an attacker begins to pay attention to the traffic and obtain useful information by collecting the session data transmitted between mobile device and its home agent. In the wireless network case, an intruder has ability to get packets transformed by radio signals. In the active eavesdropping case, the attacker prepares independent linkages with the victims and transfers messages, causing them to believe that they are directly talking to each other over a private connection, while indeed the whole conversation is directed by the attacker. The attacker should have the ability to intercept all messages among the two victims and inject new ones, that is straightforward in several situations [28].

4.9 Stolen-verifier

An attacker may thieve verification table if the scheme of authentication saves this table with LMA or MAG [26]. In order to protect the Proxy Mobile IPv6 versus this attack, AAA server does not have an obligation to save any verified information. Even though any attacker infiltrates into the AAA server database, she/he cannot obtain any user authentication information [29].

■7.0 CONCLUSION

The Proxy Mobile IPv6 is proposed to support mobility that does not require a mobile node to involve in mobility-related signaling. However, this protocol decreases latency and packet loss compared to a host-based approaches; it still suffers from security issues. An authentication is an essential part to protect this approach against different security threats. In this paper, the security criteria and various attacks are explored and analyzed to evaluate authentication approaches in Proxy Mobile IPv6. The authentication methods should be assessed based on security criteria and must be strength enough against various attacks that are discussed in this paper to find and solve current security issues.

Acknowledgement

This research is in affiliation with Ministry of Higher Education, Universiti Teknologi Malaysia, Malaysia-Japan International Institute of Technology (MJIIT) and Communication System and Network (CSN) research group.

References

[1] Soto, I., Bernardos, C. J., Calderón, M., and Melia, T. 2010. PMIPv6: A Network-based Localized Mobility Management Solution. *The Internet Protocol Journal*. 13(3) 2–15.

[2] Johnson, D., Perkins, C., andArkko, J. 2004. RFC 3775: Mobility support in IPv6. *IETF*.

[3] Mphil, N. G., and Sc, N. R. M. 2014. A Survey on Mobility Management Protocols for Improving Handover Performance. 10(1): 53–57.

[4] Soliman, H., Bellier, L., Elmalki, K., and Castelluccia, C. 2008. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management.

[5] Koodli, R. 2009. Mobile IPv6 Fast Handovers.

[6] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B., andLeung, K. 2008. Proxy Mobile IPv6. 1–92.

[7] Ki-Sik, K., Wonjun, L., Youn-Hee, H., Myung-Ki, S., and Heung Ryeol, Y. 2008. Mobility Management for all-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6. *Wireless Communications, IEEE*. 15(2): 36–45.

[8] Modares, H., Moravejosharieh, A., Lloret, J., and Salleh, R. B. 2014. A Survey on Proxy Mobile IPv6 Handover.

[9] Jiang, Q., Ma, J., Li, G., and Ye, A. 2012. Security Enhancement on an Authentication Method for Proxy Mobile IPv6. In L. Jiang (Ed.). *Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering (ICCE2011) November 19-20, 2011, Melbourne, Australia*Springer Berlin Heidelberg. 110: 345–352.

[10] Modares, H., Moravejosharieh, A., Lloret, J., and Salleh, R. 2014. A Survey of Secure Protocols in Mobile IPv6. *Journal of Network and Computer Applications*. 39(0): 351–368.

[11] You, I. 2012. *Design and Analysis of Mobile Internet Security Protocol by Using Formal Verification Methodology*. (Ph.D), Kyushu University, Japan.

[12] Hsiang, H.-C., andShih, W.-K. 2009. Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. *Computer Standards & Interfaces*. 31(6): 1118–1123.

[13] Liao, Y.-P., and Wang, S.-S. 2009. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. *Computer Standards & Interfaces*. 31(1): 24–29.

[14] Das, M. L., Saxena, A., andGulati, V. P. 2004. A Dynamic ID-based Remote User Authentication Scheme. *Consumer Electronics, IEEE Transactions on*. 50(2): 629–631.

[15] Taha, S., and Xuemin, S. 2011, 5-9 Dec. 2011. *Anonymous Home Binding Update Scheme for Mobile IPv6 Wireless Networking*. Paper presented at the Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE.

[16] Truong, T.-T., Tran, M., and Duong, A.-D. 2012. *Robust Mobile Device Integration of a Fingerprint Biometric Remote Authentication Scheme*. Paper presented at the 26th IEEE International Conference on Advanced Information Networking and Applications, AINA 2012, March 26, 2012–March 29, 2012, Fukuoka, Japan.

[17] Joong-Hee, L., Jong-Hyouk, L., and Tai-Myoung, C. 2008. *Ticket-Based Authentication Mechanism for Proxy Mobile IPv6 Environment*. Paper presented at the Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on. 26–31 Oct. 2008.

[18] Debiao, H., Jianhua, C., and Jin, H. 2012. An ID-based Client Authentication with Key Agreement Protocol for Mobile client–server Environment on ECC with Provable Security. *Information Fusion*, 13(3): 223–230.

[19] Zubair, M., Kong, X., Mahfooz, S., andJamshed, I. 2014. SIDP: A Secure Inter-Domain Distributed PMIPv6. *International Journal of Information and Electronics Engineering*. 4(2): 103–110.

[20] Tsai, J.-L., Lo, N.-W., and Wu, T.-C. 2012. *Secure Anonymous Authentication Protocol with Unlinkability for Mobile Wireless Environment*. Paper presented at the 2012 International Conference on Anti-Counterfeiting, Security and Identification, ASID 2012, August 24, 2012–August 26, 2012, Taipei, Taiwan.

[21] Haddad, W., Krishnan, S., Dupont, F., Bagnulo, M., andTschofenig, H. 2006. An Anonymity and Unlinkability Extension for OMIPv6. *Work in Progress, Draft-haddadprivacy-omipv6-anonymity-01*.

[22] Tuncer, H., Mishra, S., andShenoy, N. 2012. A Survey of Identity and Handoff Management Approaches for the Future Internet. *Computer Communications*. 36(1): 63–79.

[23] Yoon, E.-J., Choi, S.-B., andYoo, K.-Y. 2012. A Secure And Efficiency ID-based Authenticated Key Agreement Scheme Based on Elliptic Curve Cryptosystem for Mobile Devices. *International Journal of Innovative Computing, Information and Control*. 8(4): 2637–2653.

[24] Hassan, M. M., and Hoong, P. K. 2011. One-time Key and Diameter Message Authentication Protocol for Proxy Mobile IPv6. *International Journal of New Computer Architectures and their Applications (IJNCAA)*. 1(3): 624–639.

[25] Kempf, J., and Vogt, C. 2007. Security Threats to Network-Based Localized Mobility Management (NETLMM).

[26] Zubair, M., Kong, X., andMahfooz, S. 2014. CLAM: Cross-layer Localized Authentication Mechanism based on Proxy MIPv6 and SIP in Next Generation Networks. *Journal of Communications*. 9(2): 144–156.

[27] Ming-Chin, C., Jeng-Farn, L., and Meng-Chang, C. 2013. SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks. *Systems Journal, IEEE*. 7(1): 102–113.

[28] Barbudhe, V. K., andBarbudhe, A. K. 2013. Mobile IPv6: Threats and Solution. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 2(6): 265–268.

[29] Im, I., and Jeong, J. 2012. Security-Effective Local-Lighted Authentication Mechanism in NEMO-based Fast Proxy Mobile IPv6 Networks. *International Journal of Digital Information and Wireless Communications (IJDIWC)*. 2(1): 86–103.