Comments on “SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks”

ABSTRACT

- Recently, Chuang et al. have introduced a secure password authentication mechanism for seamless handover in Proxy Mobile IPv6 (SPAM). SPAM aimed at providing high-security properties while optimizing the handover latency and the computation overhead. However, it is still vulnerable to replay and malicious insider attacks, as well as the compromise of a single node. This paper formally and precisely analyzes SPAM based on the Burrows–Abadi–Needham logic, followed by its weaknesses and related attacks.

EXISTING SYSTEM

- Recently, Proxy Mobile IPv6 (PMIPv6), which is a dominant network-based IP mobility management standard, has been powered by Fast Handovers for PMIPv6 (F-PMIPv6) in a way that its long handover latency and packet loss are reduced with the help of layer-2 triggers and tunneling. However, F-PMIPv6 still suffers from its considerable handover latency due to the full authentication procedure based on the authentication, authorization, and accounting (AAA) security infrastructure. That is why during the full procedure, it is necessary for a mobile access gateway (MAG) to consult an AAA authentication server (AS) to authenticate a mobile node (MN). Several authentication schemes have been proposed to optimize the authentication.

PROPOSED SYSTEM

- This paper formally and precisely analyzes SPAM based on the Burrows–Abadi–Needham logic, followed by its weaknesses and related attacks.
- The work in proposed a ticket-based approach to solve the problem, which was then improved by the work in with the help of the tunneling between MAGs. Reference tried to optimize the latency by using a public key method. In 2013, Chuang *et al.* proposed a secure password authentication mechanism for seamless handover in PMIPv6 (SPAM), which attempted to provide high-security properties and to minimize the handover performance without the involvement of an AS. However, it is found that SPAM is susceptible to replay and malicious insider attacks while not protecting against the compromise of a single node.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

CONCLUSION

- This paper has formally analyzed SPAM with the BAN logic while pointing out its weaknesses.1According to the analysis, GK and Kas, which are shared among MAGs, cause this protocol to suffer from the compromise of a single node. In addition, SPAM is vulnerable to a replay attack due to being unable to check the freshness of n1 and b. Moreover, in the protocol, malicious MNs can launch passive and active attacks by using their security parameters, i.e., c and d. That is why all the MNs' b, c, and d, which are derived from Kas, are the same.

REFERENCE

[1] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, “SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks,” *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” RFC 5213, Aug. 2008.

[3] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, “Fast handovers for proxy mobile IPv6,” RFC 5949, Sep. 2010.

CONTINUE

[4] C. Perkins and P. Calhoun, “Authentication, Authorization, and Accounting (AAA) registration keys for mobile IPv4,” RFC 3957, Mar. 2005.

[5] J.-H. Lee, J.-H. Lee, and T.-M. Chung, “Ticket-based authentication mechanism for proxy mobile IPv6 environment,” in *Proc. 3rd ICSNC*, Sliema, Malta, Oct. 2008, pp. 304–309.

[6] J.-H. Lee and J.-M. Bonnin, “HOTA: Handover optimized ticketbased authentication in network-based mobility management,” *Inf. Sci.*, vol. 230, pp. 64–77, May 2013.