Abstract

With the development of e-commerce, ssl protocol is more and more widely applied to various network services. It is one of key technologies to keep user's data in secure transmission via internet.

This document majorly focuses on sslstrip which generates the most recent attack in the secure network connections. It strips out all the secure connections to unsecure plain connection.

In this article we depict this attack and to nullify it, we have proposed a technique cum practical
solution to strengthen data security by developing mozilla-firefox add-on and servlet code which will strengthen our defense against the https hijacking attacks.

Reference

- Peter Burkholder, “SSL Man-in-the-Middle Attacks”, SANS Institute InfoSec Reading, 2003.
- Michael Howard, “Man-in-the-Middle Attack to the HTTPS Protocol”, IEEE computer society, 2009, pp.78-81.
- Marlingspike Moixe, “New Tricks For Defeating SSL in Practice”, BlackHat Conference, USA(2009).
- Haidong Xia and Jose Carlos Brustolonl, “Hardening Web Browsers Against Man-in-the-Middle and Eavesdropping Attacks”. Proc. 14th Int’l Conf. World Wide Web(IW3C2), ACM Press, 2005, pp. 489-498.
- Thawatchai Chomsiri, “HTTPS Hacking Protection”, 21st International Conference on Advanced Information Networking and Applications Workshops(AINAW), 2007.
- Andre Adelsbach and ebatian Gajek, “Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures", Proceedings of the 1st Information Security Practice and Experience Conference, Singapore, 11-14 April, 2005.
- Moxie, Sslstrip. http://www.thoughtcrime.org/software/sslstrip/.
- http://www.mozilla.org/projects/security/pki/nss/ssl/traces/trc-clnt-ex.html A SSL research group owned by mozila.

Index Terms

Computer Science  Security

Key words

SSL Strip prevention
secure SSL

prevent attacks on SSL

prevent MITM attack
