Improving the security of Internet exchanges

March 20 2009

(PhysOrg.com) -- TLS is the main protocol used today to secure exchanges over the Internet. The protocol has been subject to attacks in recent years, resulting in identity theft and data tampering. To address these problems, Mohamad Badra, CNRS researcher at LIMOS (France), has worked in collaboration with the Ineovation company to develop two new extensions to the TLS protocol. These standards were recently published by the Internet Engineering Task Force, an international community which develops Internet standards. These are available to programmers and software vendors for use in information systems.

The SSL/TLS protocol was developed in 1995 by Netscape and has become the main protocol used worldwide to secure exchanges and transactions over the Internet (e-commerce, banking, online auctions, electronic voting, etc.). Due to problems related to the encryption algorithms used by TLS, the protocol has several major drawbacks, notably concerning collision attacks. This also raises concerns about authentication based on digital certificates. In association with Ineovation, Mohamad Badra—CNRS researcher at the Laboratoire d'information, de modélisation et d'optimisation des systčmes in Clermont-Ferrand, France—has developed two new extensions to the TLS protocol in order to improve its security.

The first extension concerns the key exchange method. A key is a parameter required to encrypt and decrypt data. Keys are either symmetric or asymmetric. With a symmetric key, the same key is used for both encryption and decryption. To ensure secure exchanges, this key must remain secret; it must be exchanged between the sender and the

receiver over a secure channel prior to the data exchange. In the case of asymmetric keys, a “public” key (known to all) is used to encrypt the data to be sent to the recipient. The recipient then uses a private (secret) key to decrypt the data. The advantage is that asymmetric keys do not require a secure channel prior to the key exchange. The extension developed by Badra uses a new method for exchanging keys, based on the association between an asymmetric algorithm and a symmetric key. A “fresh” key is therefore generated at the start of each session, and authenticated by the symmetric key. This new method is more reliable and more secure than the current method. It simplifies the deployment of TLS in network equipment, notably wireless devices and for access providers (as opposed to asymmetric keys, more complex to implement).

The second extension concerns the data hashing function. This function transforms the message into a message digest, i.e. a fairly short series of characters which represent the message. The slightest change to the message requires a change to the message digest. Furthermore, it is very difficult to reconstruct the original message based on the message digest. Hash functions are used both to ensure data integrity (HMAC functions(8)) and for the digital signature. In the first case, once the recipient receives the message, he calculates its HMAC value and checks that it matches the value transmitted by the message sender.

In the second case, the sender wishing to transmit a signed message must first calculate the message digest and then sign (encrypt) the digest using his private key. The recipient uses the sender's public key to decrypt the message digest and checks that it matches the key calculated by the recipient. Since 2005, the most commonly-used hash functions (notably MD5) have been subject to “collision attacks”, i.e. two different messages could have identical message digests, which brings into question the digital signature authentication used with the TLS protocol. The second extension developed by Badra uses new hash functions which provide better protection against collision attacks.

More information:

SSL/TLS protocol

www.ietf.org/rfc/rfc5246.txt

New extensions to SSL/TLS protocol:

www.rfc-editor.org/rfc/rfc5487.txt
www.rfc-editor.org/rfc/rfc5489.txt (active link to publication)

Other ongoing standardization work at LIMOS:

TLS client identity protection and VPN services
www.ietf.org/internet-drafts/d … ty-protection-08.txt
ftp.ist.utl.pt/pub/drafts/draf … a-hajjeh-mtls-04.txt

Provided by CNRS