Patch for flaw in key Internet protocol

January 15 2010, by Lin Edwards

Internet map as of 16th January. Image: Internet Mapping Project, Bell Labs/Lumeta Corporation

(PhysOrg.com) -- A flaw was found in November in a key Internet protocol that encrypts most sensitive online transactions and communications, including credit card and banking transactions. A patch has now been developed by the Internet Engineering Task Force (IETF), but it may take some time to be fully implemented.

The flaw is in the Transport Layer Security (TLS) protocol, which is the IETF term for the Secure Socket Layer (SSL) protocol. SSL/TLS is built into Web servers and browsers to protect sensitive information. The flaw was found by Steve Dispensa and Marsh Ray of an authentication

company in Kansas called Phone Factor, and allows an attacker to hijack and insert commands into the start of the encrypted conversation between a web browser and the web server.

The flaw exploits a feature of TLS that allows a web server to change some parameters of an encrypted session while the session is in progress. This has serious implications, as demonstrated on Twitter by one researcher. who demonstrated it could be used to order the server to reveal the victim's password. It could also potentially be used to draw money out of a victim's bank account.

One of the authors of the draft security extension for the protocol, Eric Rescorla, said the flaw in TLS shows how difficult it is to design security protocols to protect communications on the Internet. The flaw could not be exploited without considerable technical knowledge on the part of the attacker, but it is still significant because servers and clients are open to attack even if they have implemented the protocol perfectly.

The IETF has not published its official Request for Comments (RFC) document for the security extension, which is to be known as the TLS renegotiation indication extension, but Ray say the fix is stable and several groups and vendors are working on implementing it.

Deployment of the fix for commercial products that include SSL/TLS will take time because much interoperability testing will be required before vendors can ship it, and it affects a large range of products. As a workaround, most vendors have simply turned off TLS renegotiation, which does not appear to have caused many problems. Some devices, such as printers and webcams will probably never be patched because they are rarely handling critical information that would make a "man-in-the-middle" attack such as this worth worrying about.

More information: Internet Engineering Task Force: www.ietf.org/