PHYS.ORG

Cryptographic attack highlights the importance of bug-free software

February 29 2012

A padlocked icon in a web-browser or a URL starting with https provides communication security over the Internet. The icon or URL indicates OpenSSL, a cryptography toolkit implementing the SSL protocol, or a similar system is being used. New research by a collaborative team has developed an attack that can circumvent the security OpenSSL should provide. The attack worked on a very specific version of the OpenSSL software, 0.9.8g, and only when a specific set of options were used.

Dr Dan Page, Senior Lecturer in Computer Science in the Department of Computer Science at the University of Bristol, and one of the collaborative team, will present a paper at the RSA conference in San Francisco today [Wednesday 29 February] about the EPSRC-funded research.

The attack worked by targeting a bug in the software. Carefully constructed messages were sent to the web-server, each of which triggered the bug and allowed part of a cryptographic key to be recovered. Using enough messages, the entire key could be recovered.

Dr Dan Page said: "Our work suggests an underlying problem. With software and hardware playing increasingly significant roles in our day-to-day life, how much can and should we trust them to be correct?

"The answer, in part at least, is a stronger emphasis on and investment in formal verification and correctness of open source software. Our research highlights the important role this topic will play for software engineers of the future."

SSL is designed to provide two guarantees. Firstly, that a web-server accessed is the one expected, and, secondly, that subsequent communication between the user and the web-server cannot be read by anyone else.

Both guarantees are important for e-commerce websites that need to manage sensitive data such as credit card details in a secure, dependable way. However, both depend on the web-server keeping various cryptographic keys secret.

OpenSSL is embedded in many platforms, particularly those based on the Linux operating system. Some operating system vendors have started to release advisories that prompt the upgrade of older versions of OpenSSL. This acts to limit any implications of an attack.

More information: 'Practical realisation and elimination of an ECC-related software bug attack?', B B Brumle, Aalto University, Finland; M Barbosa, Universidade do Minho, Portugal; D Page, University of Bristol, and F Vercauteren, Katholieke Universiteit Leuven, Belgium, Cryptology ePrint archive: report 2011/633.

Provided by University of Bristol

Citation: Cryptographic attack highlights the importance of bug-free software (2012, February 29) retrieved 28 April 2024 from https://phys.org/news/2012-02-cryptographic-highlights-importance-bug-free-software.html