Team Prosecco dismantles security tokens

June 27 2012, by Nancy Owano

RSA SecurID SID800 Authenticator Token

(Phys.org) -- As password systems alone prove inadequate to protect information on computers against hackers, security customers have taken the advice of vendors to step up to tokens, those online security credentials that add an extra layer of protection at login. The token is designed to generate a six-digit security code that is unique to the person's credential. The rise of two-factor authentication has been accepted as the way to go for governments and corporations trying to bolster their information security. This week, though, leading token vendors are hearing news they can do without.

An international team of computer scientists figured out how to extract the keys from RSA's SecurID 800 model in as few as thirteen minutes.

The token heists were performed by a group calling themselves Team Prosecco. If they could figure the way to break in so quickly, then that places troubling questions about the efficiency of cryptographic keys being used to log into sensitive corporate and government networks, the

kinds of keys stored on “hardened” security devices used by governments and businesses.

One argument often heard among security vendors defending their token systems is that attempts, though possible, would take so long and be so difficult that risks are minimal.

The team reports that their token attack also works against older versions of the Estonian national ID card. In the case of the Estonians ID system, they were able to figure out how to forge a digital signature in about 48 hours.

Their method consisted of both modifying and improving the “Bleichenbacher” attack on RSA PKCS#1v1.5 padding.

Bleichenbacher's padding oracle attack was published in 1998. The method they use is called the “padding oracle attack.” It involves slightly modifying encrypted text thousands of times. If the system views the extra padding as a valid encryption, the attacker learns something about the original text until eventually the whole thing becomes known.

As the researchers report, “We show how to exploit the encrypted key import functions of a variety of different cryptographic devices to reveal the imported key. The attacks are padding oracle attacks, where error messages resulting from incorrectly padded plaintexts are used as aside channel.”

When the oracle (server) responds, it leaks data that may allow attackers to decrypt messages without knowing the encryption key. The team has refined the method to the point where the number of calls is significantly reduced to reveal the key.

The attack also works against other widely used security tokens than just

that one particular model, SecurID 800, from RSA. All of the companies involved were notified before the paper was published, says the research team.

RSA's SecurID 800 model took the shortest time to open at thirteen minutes. A device model made by Siemens took 22 minutes. A device model made by Netherlands-based Gemalto took 92 minutes.

The researchers will be describing their successful exploits in a paper presented at the CRYPTO 2012 (the 32nd International Cryptology Conference) in Santa Barbara, California, in August. The accepted paper is titled "Efficient Padding Oracle Attacks on Cryptographic Hardware." The document is an Inria (the French National Computer Science Research Institute) study.

Not all security watchers, however, are convinced that the study is useful. An RSA blog posting, written by Sam Curry, said "Don't believe everything you read," and that "Your SecurID Token is Not Cracked." He went on to say that "This is not a useful attack. The researchers engaged in an academic exercise to point out a specific vulnerability in the protocol, but an attack requires access to the RSA SecurID 800 smartcard (for example, inserted into a compromised machine) and the user's smartcard PIN. If the attacker has the smart card and PIN, there is no need to perform any attack, so this research adds little additional value as a security finding."

© 2012 Phys.Org

Citation: Team Prosecco dismantles security tokens (2012, June 27) retrieved 25 April 2024 from https://phys.org/news/2012-06-team-prosecco-dismantles-tokens.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.