Researchers find weakness in RSA authentication - common digital security system

March 3 2010

The most common digital security technique used to protect both media copyright and Internet communications has a major weakness, University of Michigan computer scientists have discovered.

RSA authentication is a popular encryption method used in media players, laptop computers, smartphones, servers and other devices. Retailers and banks also depend on it to ensure the safety of their customers' information online.

The scientists found they could foil the security system by varying the voltage supply to the holder of the "private key," which would be the consumer's device in the case of copy protection and the retailer or bank in the case of Internet communication. It is highly unlikely that a hacker could use this approach on a large institution, the researchers say. These findings would be more likely to concern media companies and mobile device manufacturers, as well as those who use them.

Andrea Pellegrini, a doctoral student in the Department of Electrical Engineering and Computer Science, will present a paper on the research at the upcoming Design, Automation and Test in Europe (DATE) conference in Dresden on March 10.

"The RSA algorithm gives security under the assumption that as long as the private key is private, you can't break in unless you guess it. We've

shown that that's not true," said Valeria Bertacco, an associate professor in the Department of Electrical Engineering and Computer Science.

These private keys contain more than 1,000 digits of binary code. To guess a number that large would take longer than the age of the universe, Pellegrini said. Using their voltage tweaking scheme, the U-M researchers were able to extract the private key in approximately 100 hours.

They carefully manipulated the voltage with an inexpensive device built for this purpose. Varying the electric current essentially stresses out the computer and causes it to make small mistakes in its communications with other clients. These faults reveal small pieces of the private key. Once the researchers caused enough faults, they were able to reconstruct the key offline.

This type of attack doesn't damage the device, so no tamper evidence is left.

"RSA authentication is so popular because it was thought to be so secure," said Todd Austin, a professor in the Department of Electrical Engineering and Computer Science. "Our work redefines the level of security it offers. It lowers the safety assurance by a significant amount."

Although this paper only discusses the problem, the professors say they've identified a solution. It's a common cryptographic technique called "salting" that changes the order of the digits in a random way every time the key is requested.

"We've demonstrated that a fault-based attack on the RSA algorithm is possible," Austin said. "Hopefully, this will cause manufacturers to make a few small changes to their implementation of the algorithm. RSA is a good algorithm and I think, ultimately, it will survive this type of attack."

More information: The paper is called "Fault-based Attack of RSA Authentication." Full text of paper: www.eecs.umich.edu/~valeria/re … ations/DATE10RSA.pdf

Provided by University of Michigan