New type of cryptography that can better resist "dictionary attacks"

August 5 2014

Cryptographers in China have have developed a new type of cryptography that can better resist so-called offline "dictionary attacks", denial of service (DoS) hacks, and cracks involving eavesdroppers. Their approach, reported in the *International Journal of Electronic Security and Digital Forensics*, extends and improves a type of cryptography that uses an intractable mathematical problem as its basis.

Public-key cryptography uses the complexity of certain mathematical problems that would take even a supercomputer many years to solve, to lock up data that only a person with the private key can unlock. Early public-key systems used the problem of finding the prime factors of a very large integer. More recent protocols exploit the problem of finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point. This is the "elliptic curve discrete logarithm problem" and is an example of a mathematical problem that is essentially impossible to solve at the highest level without an array of supercomputers and tens of thousands of years at one's disposal. And, yet, it is very efficient in terms of computation to implement and encrypt data.

Unfortunately, encryption systems always have loopholes and can always succumb to bugs or attacks on the computer system on which they run. The most recent form of elliptical encryption widely used for internet logins and other applications can be breached by a so-called offline dictionary attack that simply tests every possible key, or password, non-complex passwords thus succumbing the quickest. More the protocol can

be attacked by an eavesdropper who monitors and replicates password entry by users or otherwise breaks the system, through a denial of service, attack allowing entry via the backdoor.

Pengshuai Qiao of North China University of Water Resources and Electric Power, in Zhengzhou, and Hang Tu of Wuhan University, Wuhan, China, explain that two fundamental requirements of secure communications over an insecure public network are password authentication and password updating. Previous researchers have extended password authentication and update schemes based on elliptic curve cryptography to the point where they are entirely robust against replay attack, man-in-the-middle attack, modification attack and other potential breaches. However, this system, developed by computer scientists Hafizul Islam of the Birla Institute of Technology and Science in Pilani and GP Biswas of the Indian School of Mines, Dhanbad, India, failed to defend against offline password guessing attack and stolen-verifier attack.

Qiao and Tu have now devised an algorithm for on elliptic curve cryptography that precludes such security breaches by using a four-phase approach: registration phase, password authentication phase, password change phase and session key distribution phase. These are the same steps used with the Islam-Biswas scheme but Qiao and Tu add two additional calculations on the user side for the final single-session password. This change means that offline dictionary attacks will never succeed because even if the hacker guesses the user's password they will not have the necessary algorithm to recalculate the actual session password used each time by the user. The same addition also thwarts stolen-verifier attacks, because even if a third-party has access to the verification protocol used by the system, they would still need to be able to do the one-time additional pair of calculations for the given session.

The team's initial testing of the new system bodes well for secure

implementation on a wide range of platforms for everything from mobile banking to web logins.

More information: Qiao, P. and Tu, H. (2014) 'A security enhanced password authentication and update scheme based on elliptic curve cryptography', *Int. J. Electronic Security and Digital Forensics*, Vol. 6, No. 2, pp.130-139. www.inderscience.com/info/inar … icle.php?artid=63109

Provided by Inderscience Publishers