Crippling crypto weakness opens millions of smartcards to cloning

Gemalto IDPrime.NET almost certainly isn't the only smartcard vulnerable to ROCA.

DAN GOODIN - 10/23/2017, 10:30 PM

HTTPS://ARSTECHNICA.COM/INFORMATION-TECHNOLOGY/2017/10/CRIPPLING-CRYPTO-WEAKNESS-OPENS-MILLIONS-OF-SMARTCARDS-TO-CLONING/

Enlarge

Gemalto

73

Millions of smartcards in use by banks and large corporations for more than a decade have been found to be vulnerable to a crippling cryptographic attack. That vulnerability allows hackers to bypass a wide range of protections, including data encryption and two-factor authentication.

FURTHER READING

Millions of high-security crypto keys crippled by newly discovered flaw

The critical vulnerability, which researchers disclosed last week, allows attackers to derive the private portion of any vulnerable key using nothing more than the corresponding public portion. The so-called factorization attack can be completed in minutes or days, and the price can range from nothing, depending on the key size and type of computer an attacker uses, to $20,000. The vulnerability stems from a widely deployed library developed by German chipmaker Infineon, which in turn sells its hardware and software to third-party smartcard and device manufacturers.

The defect has now been confirmed to affect the first line of Gemalto IDPrime.NET smartcards. The cards have been on the market since 2004 at the latest, when Gemalto predecessor Axalto announced Microsoft employees were using the card to secure access to the software maker's network, by, among other things, providing two-factor authentication to company employees worldwide. During the 12 years the cards are known to have been in use, Netherlands-based Gemalto has shipped cards numbering in the millions or even the tens or hundreds of millions.

Gemalto stopped selling the product in September, but it has pledged to support them for 24 to 48 months after that, depending on how the cards are used. Third-party distributors continue to sell the cards online. A Gemalto representative referred Ars to this company advisory that says: "Our investigation has determined that End-of-sale IDPrime.NET products may be affected."

Cryptography experts, however, said there is little doubt the line of Gemalto cards is affected. Dan Cvrcek, CEO of Enigma Bridge, said he examined 11 IDPrime.NET cards issued from 2008 through earlier this year. All of them used an underlying public key that tested positive for the crippling weakness. By running the public keys through an attack hosted on Amazon Web Services or a similar cloud computing platform, the private portions could be computed in a matter of hours for 1024-bit keys and in a matter of days for 2048-bit keys. Once attackers know the secret key, they could cryptographically clone the card. Attackers could also compromise any other keys that were generated by the smartcards.

Keys to the kingdom

Cvrcek said members of the research team that discovered the flaw went on to obtain two RSA keys with a length of 512 bits that were generated by separate IDPrime.NET cards. His team was able to calculate the secret key for both of them, one in about three minutes and the other in about 10 minutes, using a general-purpose computer. He said the results are alarming, because they confirm the weakness affects a card that forms the basis for a public key infrastructure many companies use to encrypt e-mail, secure network logins, and authenticate employees.

"These card were primarily used for enterprise and medium-sized company PKI systems, Cvrcek said. "They are protecting e-mail communication, remote access (VPN), they are used to sign and decrypt sensitive documents. The documents would likely be highly sensitive ones—whatever an enterprise gives maximum confidentiality level."

Gemalto's IDPrime.net card is only the latest smartcard to be confirmed vulnerable to ROCA, and it almost certainly won't be the last one. Estonia's government has already said that 750,000 electronic IDs it has issued are vulnerable, and researchers have uncovered evidence ID cards issued by Slovakia and Spain may be vulnerable, too. Several models of Trusted Platform Modules protecting computers sold by a variety of manufacturers are also known to be affected, as are Javacards.

The vulnerability resides in all RSA keys generated by the faulty Infineon library. To optimize speed, the library uses a structure of underlying prime numbers that makes the keys much more susceptible to a mathematical process known as factorization. Identifying affected keys is quick and inexpensive and requires only access to a public key. Attackers can then run all vulnerable public keys through an attack dubbed Return of the Coppersmith Attack, or ROCA, for the type of factorization method it uses.

Once the longer factorization is completed, attackers have access to the private key that's used for a variety of sensitive tasks, including decrypting data, digitally signing software, and providing a cryptographically robust second authentication factor. The attack and the vulnerability it exploits were discovered by Slovak and Czech researchers from Masaryk University in the Czech Republic, Enigma Bridge in Cambridge, UK, and Ca' Foscari University in Italy. Cvrcek said other lines of Gemalto smartcards, including the IDPrime MD, aren't vulnerable.

Now that the IDPrime.NET has been confirmed to be affected, organizations that use the smartcard should carefully assess how their networks and employees can be exploited. A Microsoft spokeswoman said company officials are investigating the vulnerable cards and will take appropriate steps if they determine there's a risk to the company's network or employees. Gemalto officials declined to say how many smartcards have been sold over the years or how many remain in active use. Cvrcek estimated sales totals in the millions at a minimum and possibly in the hundreds of millions. It's not hard to find case studies naming specific companies that use the Gemalto cards. This one, for instance, shows that British Sky Broadcasting Group recently deployed vulnerable cards to 4,000 employees.

DAN GOODIN Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.**EMAIL** dan.goodin@arstechnica.com // **TWITTER** @dangoodin001