Flaw crippling millions of crypto keys is worse than first disclosed

Estonia abruptly suspends digital ID cards as crypto attacks get easier and cheaper.

DAN GOODIN - 11/6/2017, 11:10 PM
HTTPS://ARSTECHNICA.COM/INFORMATION-TECHNOLOGY/2017/11/FLAW-CRIPPLING-MILLIONS-OF-CRYPTO-KEYS-IS-WORSE-THAN-FIRST-DISCLOSED/

Enlarge / A digital identity card issued by the Republic of Estonia.

Republic of Estonia, Interior Department

73

A crippling flaw affecting millions—and possibly hundreds of millions—of encryption keys used in some of the highest-stakes security settings is considerably easier to exploit than originally reported, cryptographers declared over the weekend. The assessment came as Estonia abruptly

suspended 760,000 national ID cards used for voting, filing taxes, and encrypting sensitive documents.

FURTHER READING

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

The critical weakness allows attackers to calculate the private portion of any vulnerable key using nothing more than the corresponding public portion. Hackers can then use the private key to impersonate key owners, decrypt sensitive data, sneak malicious code into digitally signed software, and bypass protections that prevent accessing or tampering with stolen PCs. When researchers first disclosed the flaw three weeks ago, they estimated it would cost an attacker renting time on a commercial cloud service an average of $38 and 25 minutes to break a vulnerable 1024-bit key and $20,000 and nine days for a 2048-bit key.

Organizations known to use keys vulnerable to ROCA—named for the Return of the Coppersmith Attack the factorization method is based on—have largely downplayed the severity of the weakness. Estonian officials initially said the attack was "complicated and not cheap" and went on to say: "Large-scale vote fraud is not conceivable due to the considerable cost and computing power necessary of generating a private key." Netherlands-based smartcard maker Gemalto, meanwhile, has said only that its IDPrime.NET—a card it has sold for more than a decade as, among other things, a way to provide two-factor authentication to employees of Microsoft and other companies—"may be affected" without providing any public guidance to customers.

FURTHER READING

Crippling crypto weakness opens millions of smartcards to cloning

Independent researchers, however, have determined the crippling weakness is present in cards issued from 2008 to earlier this year.

On Sunday, researchers Daniel J. Bernstein and Tanja Lange reported they developed an attack that was 25 percent more efficient than the one created by original ROCA researchers. The new attack was solely the result of Bernstein and Lange based only on the public disclosure information from October 16, which at the time omitted specifics of the factorization attack in an attempt to increase the time hackers would need to carry out real-world attacks. After creating their more efficient attack, they submitted it to the original researchers. The release last week of the original attack may help to improve attacks further and to stoke additional improvements from other researchers as well.

International cybercrime networks, take note

In an e-mail, Dan Cvrcek, CEO of Enigma Bridge, one of the outside organizations that helped in the original research, said he, too, believes much faster and less expensive attacks are possible.

One way to improve the attack, Bernstein and Lange said, may be to use fast graphics cards, which have the potential to shave the average cost of factorizing a vulnerable 2048-bit key to $2,000 in energy costs.

"My impression is that the time and cost estimates cited in the original research have been fairly conservative," he wrote. "I'm not sure whether someone can slash the cost of one key below $1,000 as of today, but I certainly see it as a possibility."

On Friday, Estonia's Police and Border Guard suspended an estimated 760,000 ID cards known to be affected by the crypto vulnerability. The country's prime minister, Jüri Ratas, said the move came as officials learned the weakness affected cards and computers around the world, not just Estonian IDs. The wider-than-expected coverage, he said, "brought the safety flaw to the attention of international cybercrime networks which have significant means to take advantage of the situation."

One of the scenarios Bernstein and Lange presented in Sunday's post is that serious attackers can further reduce costs by buying dedicated computer gear, possibly equipped with GPU, field programmable gate array, and application-specific integrated circuit chips, which are often better suited for the types of mathematical operations used in factorization attacks. The estimates provided by the original researchers were based on the cost of renting equipment, which isn't as cost-effective when factorizing large numbers of keys. They also noted that compromising just 10 percent of cards used in country-wide voting might be enough to tip an election.

This weekend's suspension affects all cards Estonia issued from October 16, 2014 to October 25 of this year. The cut-off is almost two months after August 30, the date researchers privately reported the vulnerability to Estonian officials. The country is now issuing cards that use elliptic curve cryptography instead of the vulnerable RSA keys, which are generated by a code library developed and sold by German chipmaker Infineon. Estonian card holders can find details on card updates here.

Estonia is almost certainly not the only country with a national ID card that's vulnerable to ROCA. Researchers said cards issued by Slovakia also tested positive for the vulnerability. Ars is also aware of unconfirmed reports of a Western European country that also issues affected ID cards. When counting smartcards used in private industry, the number of vulnerable keys may reach into the tens or hundreds of millions, and possibly more. As the numbers grow higher, it won't be surprising if the time and cost of carrying out attacks continues to drop.

Post updated to correct the location of Gemalto and to remove incorrect statement about a revised attack.

Promoted Comments

- Fatesrider Ars Scholae Palatinae *et Subscriptor*

JUMP TO POST

afidel wrote:

$1,000 per voter? No, it's not going to lead to election fraud, even in the US where we have insane campaign spending the cost per vote is around $10 per vote in federal elections and $30 per vote in statewide elections. Nobody is going to spend 30-100x as much on a fraudulent vote as they are on legitimate votes through campaigning.

However some of the other uses do seem like they'd be big targets for such a cheap attack.

You misunderstand how to do something like that.

All you need to do is close the poll margin with a small, but significant, margin of error. Usually, that's no more than 5% of the total votes. One doesn't need to hack EVERYONE to do that. Just the side that you don't want to win, so you're even lower than 5% of the total (since a 2.5% swing from one side to the other will result in a 5% margin difference since it REMOVES those votes from one side lowering their amount by 2.5% and gives them to the other, increasing theirs by 2.5%).

That puts this firmly in the "affordable" category, whether or not the person so affected even votes. It's better to find a 131 year old Floridian kind of situation to hack than a live person, but it certainly can be done AFTER the fact to change votes once cast depending on how that system works.

This is why I have always insisted that no electronic machine be used to accept or count votes. The integrity of the vote is more important than "convenience", and the U.S. is proving that the electronic voting system is seriously flawed when you can't even tell if your voting machine has been tampered with.

6237 posts | registered 11/16/2012

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