ROCA: BLAMING INFINEON IS THE EASY WAY OUT

Oct 26, 2017 | by Ingo Schubert

https://www.rsa.com/en-us/blog/2017-10/roca-blaming-infineon-is-the-easy-way-out

This is going to hurt a little: *You can do everything right and still screw up majorly*.

Many of you read about the Infineon crypto module flaw. The story has been reported with variations of on the theme of “RSA algorithm weakness in Infineon chips”.

First, let’s get this right. This was *not* about a weakness in the RSA® algorithm, nor was it about Infineon’s implementation of the algorithm. Infineon did that part just fine.

The problem occurred in the way Infineon generated the prime numbers used as key material. They took shortcuts to produce the key material prime numbers, because without those shortcuts the generation of the primes would simply take too long.

“That’s stupid and irresponsible!” some may scream. As if it would be that simple. There are valid reasons to speed up prime number generation on embedded devices (Smartcards, TPM chips) used directly by end-users. The chips lack CPU power as their main job is to protect the key material, not to run video games.

When generating RSA keys (and, therefore, primes) on thousands of devices it had better be fast; people don’t like to wait. The crypto-aware end-user understands that key generation can take time, but many others will simply yank the smart card out of the reader because it “hangs”.

Using shortcuts in RSA implementations is a very common practice. For example, people often choose encryption exponents like 3, 17, or 65,537 because they lend themselves to much faster computation. In some implementations, these choices have proven problematic, but on the whole, they have proven to be a sound way to implement the RSA algorithm in practice. Like any cryptographic approach, these choices have to withstand the test of time.

It’s worth noting that these attacks are not obvious. It requires some fairly ingenious observations made by some incredibly smart people. Cryptography is hard. Implementing it correctly is even harder. On the surface, it seems that Infineon likely exercised good diligence and correctly implemented an approach for fast prime generation. This approach was only recently discovered to have a subtle, but critical, mathematical flaw. This is not the typical “I invented my own crypto!” story.

Yet here Infineon sits, after selling truckloads of chips with the faulty key generator.

Two things stand out to me:

1. The problem is substantial as the attack could be performed by anyone with few resources, or know-how. All you need is the public key and some CPU time. Both are pretty easy to come by.
2. The smart card chip plus firmware was certified to Common Criteria EAL 5+, which is a pretty extensive certification. The TPM module certified EAL 4+, which is also pretty high.

Looking at the Common Criteria website, which lists all certified products, there are several Infineon chips and libraries included. While I am not sure this is the exact chip in question it serves well as an example for the points I make below. This Infineon chip was certified to EAL5+.

Some may be shocked that this flaw could slip thru such an extensive certification process. Understanding how certifications actually work removes the shock factor.

Certifications, such as Common Criteria EAL, do not certify that the product doing function X is secure in every possible way. It certifies that function X was implemented in a secure way. These are not the same thing.

Additionally, there can be confusion as to what is certified. Certifications are about the “Target of Evaluation” (ToE), which describes what will be certified. Everything not mentioned in the ToE is *not* included in the evaluation, even if it is closely related. In the example evaluation linked to above, the random number generator is included in the ToE, but there is no mention of the prime number check. It may be somewhere in the ToE, but remember, the certification is about the secure implementation of function X and not about the security of X itself.

In other words: the security of the “fast prime” functionality – even if included in the – ToE was never part of the evaluation.

This should serve as a stark reminder that certification stamps, such as Common Criteria, FIPS and so on, do not mean the product is secure. Nor does it mean that installation of a certified product equals a secure deployment. It only means what the ToE explicitly states.

Infineon released a patch to end users via device and OS manufacturers for the TPMs. The smart cards need to be physically replaced. As with most patches, this patch won’t be installed immediately on every system and it takes time to reissue affected smart cards leaving a large attack window. Combined with the fact that some use cases for the affected smart cards involve digital signatures and that timestamping a legally binding digital signature is not yet mandatory, this could get interesting. One scenario could have an attacker deriving the private key sometime in the future to create valid signatures on documents (e.g. contracts). Due to the lack of timestamps it cannot be proven they were created after the compromised certificate had been revoked.

PKI (Public Key Infrastructure) and cryptography aren't easy. Hindsight allows us to say where Infineon went wrong, but at the time the decisions were made things simply looked OK. Most of us would have made the same decision in that position.

Any cryptographic algorithm must withstand the test of time. As the oldest public-key cryptosystem, the RSA algorithm has withstood that test for the better part of 40 years. One should, therefore, continue to have confidence in it knowing that it has been thoroughly examined for so long, and continues to be used. Newer algorithms, as promising as they may seem, can be more risky since they may contain issues yet to be unearthed.

Author: Ingo Schubert
Category: RSA Point of View
Keywords: algorithm, Cryptography, Digital Signature, Infineon, smart card, TPM