

FS-2009-03

Possible Leakage of Encrypted Information When Using RSA-CRT in Smartcards

Smartcards are used in an increasing number of applications: examples of the daily use of smartcards are sim-cards in cellphones, chips on bank cards and access cards for buildings. An important use of smartcards is the possibility to safely store and communicate user data or permissions. Smartcards can be used to encrypt data.

Researchers of the Dutch company Riscure have discovered a new variant of an existing attack method, with which certain smartcards will release information on the cryptographic keys when they are being analyzed. Certain measures in the way the cryptographic functions are implemented prevent these attacks. This factsheet briefly describes the discovered vulnerability, it indicates how you can find out if your smartcard is vulnerable, and lets you know what could happen upon compromise and which measures you can take in order to reduce the risk if that should be the case.

The Vulnerability

Smartcards can be implemented using various types of encryption, RSA being one of them. RSA is a strong encryption-algorithm that uses separate keys for encrypting and decrypting information. This is known as *asymmetric encryption*. The key that is used to decrypt data is the *private* key and needs to be kept a secret, the key that is used to encrypt data is the *public* key. Public and private key pairs are also used to generate and verify digital signatures of information, so as to allow the reader to verify the integrity of the information. The key-length determines the time that is required to guess the key. Keys with a length of 1024 bits are considered to be strong considering the technology that is currently in use. Often keys of 2048 bits are in use. RSA is widely used all over the world.

Asymmetric encryption generally costs more computing power and memory than symmetric encryption, in which technique the same key is used for both encrypting and decrypting information. These resources are scarce on a smartcard. The RSA-calculation that requires the private key (decrypting encrypted information or digitally signing it) can be implemented efficiently by using the *Chinese Remainder Theorem* (CRT) algorithm. This much-used RSA-implementation enables the calculations to be done four times faster than the standard implementation. Various RSA-CRT implementations now appear to be vulnerable for a new variant of the so called side channel attack. Researchers have managed to extract the secret RSA-key from specific smartcards in only a few hours in a laboratory setup. This attack requires measuring equipment that is freely available in the marketplace for several thousand Euros.

In order to perform this attack, the attacker needs to have the smartcard do a great number of RSA-decryptations (or generate many RSA-signatures) and to monitor the power consumption of each of these operations. The attacker needs to have possession of the smartcard for only several hours.

There is a number of well-known measures that can be used to protect an RSA-CRT implementation and to prevent this problem.

An overview of the facts:

- > Smartcards are used in bank cards, access cards for buildings and SIM-cards in cellphones
- > They protect sensitive information and are therefore continuously improved to resist new types of attacks.
- > Smartcards that use RSA-cryptography, implemented by use of the CRT-algorithm may be vulnerable for a new type of an existing attack.
- > An attacker that manages to obtain the RSA-keys can copy the smartcard and use it to decrypt communication or digitally sign messages. This can lead to greater or smaller damage, depending on the application of the technology.
- > If you use smartcards, you should consider the risks of being vulnerable to the attack. This factsheet provides pointers to do so.

The Anatomy of Such an Attack

Generally speaking, guessing or breaking cryptographic keys is easier when the number of possible keys is limited by any additional information the attacker has on the applied encryption algorithm. This information can be gathered by means of a so-called *side-channel* attack. This type of attack entails analyzing the external behaviour of the smartcard, such as heat radiation, power consumption or electromagnetic emission.

In the case of this attack, the CRT-algorithm is studied by analyzing the electric load on the smartcards chip, while it is in use. While processing the input, certain steps in the process consume more power than others. By varying the input and monitoring the subsequent power consumption, the attacker can make assumptions about the keys that have been used. The goal of this type of attack is to reduce – by analyzing power consumption – the number of possible private keys, so as to discover the actual key in as little time as possible.

What is the Risk?

- An attacker who is able to extract secret RSA-keys is able – even when he no longer has possession of the physical card – to decrypt communication that usually can only be decrypted by means of the smartcard or generate digital signatures that can only be generated with the smartcard. This can lead to greater or smaller damage, depending on the application of the technology. Leakage of cryptographic keys can compromise the confidentiality and integrity of the information that was either encrypted or digitally signed by these keys.

When are you at Risk?

Not all smartcards that use RSA-encryption are vulnerable and the RSA-algorithm itself has not been broken. Additionally, not all CRT-implementations are vulnerable. In order to find out whether your smartcard application is vulnerable it is best to first contact your smartcard-supplier. He has been notified of the vulnerability. Should you receive insufficient support or information, you can check whether you are vulnerable by taking the steps below:

1. Check whether your smartcard uses RSA. If this is not the case, you are not vulnerable for this attack vector.
2. Check whether RSA was implemented by using CRT. If this is not the case, you are not vulnerable for this attack vector.
3. Have your smartcard tested. In order to do so, you can contact – amongst others – Riscure or Brightsight – both are located in Delft.

Protection against the Risks and Actions You can Take

If your smartcard uses a vulnerable RSA-CRT implementation, there are a number of measures you can take to decrease the risk you are exposed to. These are largely the same as the measures that are described in GOVCERT.NL factsheet FS-2008-003 *Vulnerabilities of Mifare Classic chips in access cards*.

- *Determine security measures already in place;*
The risk of keys being extracted from vulnerable smartcards can be decreased by using additional security measures. One of the possible measures is to protect the cryptographic functions with a PIN-code. When the smartcard does not perform any calculations, an attacker cannot analyze the card's power consumption. This reduces the risk of this vulnerability being exploited. Note, however, that having the card and the PIN is enough for an offender to reach his goal. Should this be the case, he will not take the trouble to go through the process of analysing the chip.
- *Evaluate the residual risk and, if necessary, take additional measures.*
Determine if the measures in place are sufficient with regard to the sensitivity of the applications or data that are protected by the smartcard. Key questions are:
 - do the measures offer sufficient security, with regard to the potential damage if the smartcard's security is broken?
 - Which other processes will be harmed should the confidentiality of the cryptographic keys be compromised and which damage could subsequently be caused?

Depending on the type of chip that is used, the use of CRT can be disabled. However, this will have an adverse effect on speed while using the chip. The afore-mentioned factsheet, FS-2008-03, mentions various additional measures. We advise you to also consult this publication.

- *Consider replacing the smartcards with a better variant.*

Depending on the effect and the cost of additional measures, it might be necessary to consider replacing the smartcards with a better variant. There is a good possibility that only the physical smartcards will need to be replaced. Please note: as replacing the smartcards can be a time-consuming activity, (temporary) additional measures are inevitable.

Additional information

- The description of the vulnerability: <http://www.riscure.com/news-events/publications.html>
- An explanation of the RSA-algorithm: <http://en.wikipedia.org/wiki/RSA>
- The GOVCERT.NL factsheet on the Mifare-chip: <http://www.govcert.nl/download.html?f=110>