EUROSMART
The Voice of the Digital Security Industry

Brussels, 16th May 2018

Eurosmart confirms that security of products and services is not impacted by the recent publication on SCP02

Eurosmart has noted the publication from Gildas Avoine (Rennes University, INSA Rennes) and Loïc Ferreira (Orange Labs) on the potential Vulnerability on the SCP02 protocol, published yesterday on the TCES Website.

This new publication reports a known attack but applied in a new context.

For a long time, Eurosmart has been recommending that additional security measures should be added to SCP02, such as e.g., pre-encrypting sensitive data, restricting the usage to trusted environments, or other means that are appropriate to enhance the security of SCP02.

Please find here below a Q&A developing more in detail the questions that you may have as Eurosmart technology end-user.

Eurosmart is committed to developing, promoting and maintaining the appropriate security level for its products, solutions and protocols.

Eurosmart Q&A:

Q1: What can we do from this attack? What we cannot do?

What is retrieved is the said plaintext (not the key) and from only one card.

A pre-encrypted data cannot be retrieved in clear.

Q2: What are the conditions to perform this attack?

The conditions for performing the attack on SCP02 are as follows:

- Attacker must be able to intercept and modify messages between server and card in open environment;
- Attacker must be able to perform precise timing measurement (wrong padding or good padding) with access either to the device or ability to load spy malware;
- The same plain text must be sent enciphered several times (around 128 times to disclose one single byte of information either to different cards with different keys or to the same card with different session keys).

Q3: What are the type of product applicable/not applicable to this attack?

Attack is **not applicable** to the electrical personalization of banking applets (all sensitive data are over encrypted).

Attack is **not applicable** if personalisation is done in a secure place (personalization place is usually certified by schemes or performed in trusted environments).

Attack is **not applicable** if personalization is done by OTA through SCP80/SCP81 secure channel.

Attack is **not applicable** over data that are encrypted using the Data Encryption Key (DEK).

Q4: What are the recommendations to be applied?

For ongoing programs using SCP02, the GlobalPlatform Security Task Force recommends the following simple rules:

- Use ICV encryption recommendation from GPC_FAQ_021;
- Encrypt all sensitive data transmitted in SCP02 using the Data Encryption Key (DEK) or any applet key;
- Disable SCP02 if there is no need to update the card in the field;
- Add SCP03 in the card platform to be able to smoothly switch to AES crypto.

Restricting the use of SCP02 to trusted environment can also be considered as a valid alternative.

As a reminder, the SCP02 Global Platform Statement is the following:

In March 2018, GlobalPlatform has issued a security informative note about the evolution of the trends related to the Secure Channel Protocol 02 (a.k.a. SCP02) specified in the Card Specification document.

GlobalPlatform organization set as **deprecated** this protocol in the current version of GlobalPlatform specification (Card Specification v2.3.1).

Refer to the GlobalPlatform recommendations as described in the informative note: https://www.globalplatform.org/documents/Security_Informative_Note1_FINAL.pdf

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

Eurosmart members are companies (Fingerprint Cards, Gemalto, Giesecke+Devrient, GS TAG, IDEMIA, IN GROUPE, Infineon Technologies, Inside Secure, Internet of Trust, Linxens, Nedcard, NXP Semiconductors, +ID, Real Casa de la Moneda, Samsung, Sanoïa, STMicroelectronics, Toshiba, Trusted Objects, WISekey, Winbond), laboratories (CEA-LETI, Keolabs), research organisations (Fraunhofer AISEC), associations (SCS Innovation cluster, Smart Payment Association, Mobismart, Danish Biometrics).

Press contact:

Pierre-Jean VERRANDO
Director of operations
Mobile: +32 471 34 59 64

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 3635 | mail eurosmart@eurosmart.com