ST33TPHF2ESPI, ST33TPHF20SPI, ST33TPHF2EI2C and ST33TPHF20I2C TPM 2.0 security recommendations

Introduction

This technical note provides the security recommendations needed to thwart the so-called lattice attack during elliptic curve digital signature algorithm (ECDSA) signature generation.

Some countermeasures at system level may mitigate the exploitability of this attack. However, removed from its operating environment, the device remains vulnerable and the upgrade of the Trusted Platform Module (TPM) firmware is the only solution to avoid the risk of private key disclosure.

This document applies to the ST33TPHF2ESPI, ST33TPHF20SPI, ST33TPHF2EI2C and ST33TPHF20I2C products loaded with the following firmware versions (where xx represents the minor version of the firmware):

- ST33TPHF20I2C and ST33TPHF20SPI with firmware 74.xx
- ST33TPHF2ESPI and ST33TPHF2EI2C with firmware 73.xx
- ST33TPHF2ESPI with firmware 71.xx.

1 Recommendations for countermeasure mitigation at system level

The ST33TPHF2ESPI, ST33TPHF20SPI, ST33TPHF2EI2C and ST33TPHF20I2C devices are based on Arm® cores.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

For products that are not upgraded with a firmware (FW) embedding the ECDSA security fix, the following recommendations must be taken into consideration.

Several countermeasures at system level can mitigate the device vulnerability exploitability.

These countermeasures must however be protected at system level and must NOT be bypassed without detection and reaction.

The possible countermeasures are:

- Limit ECDSA key usage by replacing the key after a fixed number of generated signatures. Thanks to this countermeasure, the lattice attack is not exploitable because of the insufficient number of generated signatures.
- Use an encryption session to enter the data to be signed in an encrypted form inside the TPM device. In this way, the attacker is not able to correlate data with signatures and timing.
- Configure access control for ECDSA key usage. The TPM device enforces a secure authorization and/or policy value to use the key provided that dictionary attack mitigation is activated. The detection of false authorizations triggers a response delay that increases the time between the trials.
- Limit the availability and accuracy of TPM command execution time measurements in a log or through the communication driver application programming interface (API).

2 Solution based on TPM firmware image updates

The TPM versions listed in the “Impacted FW version” column of Table 1. Impacted TPM products vs fixed firmware images are identified as vulnerable.

The correction is embedded in several versions of FW depending on the communication interface (SPI/I²C interfaces) and the version of the TCG TPM 2.0 specification on which the FW is based (revisions 1.16 and 1.38, see [TPM 2.0 r116] and [TPM 2.0 r138], respectively).

2.1 Impacted products and fixed FW images based on the same TPM 2.0 specification

The following table lists the versions of TPM FW that embed the correction, and the corresponding products that can be field-upgraded based on the same TCG TPM 2.0 specification.

Table 1. Impacted TPM products vs fixed firmware images

Product name	Ordering code[1]	Impacted FW version	FW image version with ECDSA security
ST33TPHF2ESPI	ST33HTPH2ExxAAE6	71.00 (0x47.00)	71.16 (0x47.10)
	ST33HTPH2ExxAHA6	71.04 (0x47.04)	
	ST33HTPH2ExxAHB6	71.12 (0x47.0C)	
	ST33HTPH2ExxAAF1	73.00 (0x49.00)	73.20 (0x49.14)
	ST33HTPH2ExxAHB4	73.04 (0x49.04)	
	ST33HTPH2ExxAHC0	73.08 (0x49.08)	73.64 (0x49.40)
ST33TPHF20SPI	ST33HTPH20xxAAF3	74.00 (0x4A.00) 74.04 (0x4A.04)	74.20 (0x4A.14)
	ST33HTPH20xxAHC1	74.08 (0x4A.08)	74.64 (0x4A.40)
	ST33HTPH20xxAHC9	74.16 (0x4A.10)	
ST33TPHF2EI2C	ST33HTPH2ExxAHB8	73.05 (0x49.05)	73.21 (0x49.15)
	ST33HTPH2ExxAHC2	73.09 (0x49.09)	73.65 (0x49.41)
ST33TPHF20I2C	ST33HTPH2ExxAHB9	74.05 (0x4A.05)	74.21 (0x4A.15)
	ST33HTPH20xxAHC3	74.09 (0x4A.09)	74.65 (0x4A.41)

1. *Where xx is 28 or 32 depending on the package (TSSOP28 or VQFN32)*

2.2 Impacted products and fixed FW images based on a different TPM 2.0 specification

Another possibility is to upgrade the impacted FW based on TCG TPM 2.0 specification revision 1.16 ([TPM 2.0 r116]) to a FW image based on TCG TPM2.0 specification revision 1.38 ([TPM 2.0 r138], with the ECDSA security fix) after a clear operation (using the `TPM2_Clear` command).

The following table lists the TPM FW versions that embed the correction, and the corresponding products embedding TPM FW with TCG TPM2.0 specification revision 1.16 ([TPM 2.0 r116]), which can be field-upgraded to TCG TPM 2.0 specification revision 1.38 ([TPM 2.0 r138]).

Table 2. Allowed migration of FW images from TCG TPM 2.0 specification revision 1.16 to revision 1.38

Product name	Ordering code[1]	Impacted FW versions based on TCG TPM 2.0 specification revision 1.16	FW image versions with ECDSA security based on TCG TPM 2.0 specification revision 1.38
ST33TPHF2ESPI	ST33HTPH2ExxAAE6	71.00 (0x47.00)	73.64 (0x49.40)
	ST33HTPH2ExxAHA6	71.04 (0x47.04)	
	ST33HTPH2ExxAHB6	71.12 (0x47.0C)	
	ST33HTPH2ExxAAF1	73.00 (0x49.00)	
	ST33HTPH2ExxAHB4	73.04 (0x49.04)	
ST33TPHF20SPI	ST33HTPH20xxAAF3	74.00 (0x4A.00) 74.04 (0x4A.04)	74.64 (0x4A.40)
	ST33HTPH20xxAHC1	74.08 (0x4A.08)	
	ST33HTPH20xxAHC9	74.16 (0x4A.10)	
ST33TPHF2EI2C	ST33HTPH2ExxAHB8	73.05 (0x49.05)	73.65 (0x49.41)
	ST33HTPH2ExxAHC2	73.09 (0x49.09)	
ST33TPHF20I2C	ST33HTPH2ExxAHB9	74.05 (0x4A.05)	74.65 (0x4A.41)
	ST33HTPH20xxAHC3	74.09 (0x4A.09)	

1. *Where xx is 28 or 32 depending on the package (TSSOP28 or VQFN32)*

Warning:

For TPM products based on TCG TPM 2.0 specification revision 1.38, it is not allowed to process field upgrades with FW images based on TCG TPM 2.0 specification revision 1.16 for compatibility reasons. See Section Appendix A Upgrade table.

3 Key renewal recommendations for the field upgrade solution

The table below gives recommendations for products that embed an impacted firmware version and use ECDSA keys in order to ensure that the key material is not vulnerable after firmware update.

Table 3. Field upgrade solution recommendations

Type of key generated on impacted product	Key hierarchy	Security recommendations
ECDSA key with `sign` attribute	Storage, Endorsement	Use the `TPM2_Clear` command to remove all the keys and NV indexes. Then, regenerate all the keys and NV indexes after field upgrade to the fixed TPM FW. Or Use the `TPM2_EvictControl` command to remove the ECDSA key. Then, regenerate the ECDSA key after field upgrade to the fixed TPM FW.
ECDSA key with `sign` attribute	Platform	Use the `TPM2_EvictControl` command to remove this key. Then, regenerate the ECDSA key after field upgrade to the fixed TPM FW. Or After field upgrade to the fixed TPM FW, generate a new key and revoke the replaced key.
Other keys	-	No impact

4 Part number roll over solution

The table below lists the orderable commercial part numbers that include the ECDSA security fix.

Table 4. New TPM products with a FW version containing ECDSA correction

Product name	Commercial part number[1]	TPM library	FW version
ST33TPHF2ESPI	ST33HTPH2ExxAHD6	1.16	73.20 (0x49.14)
	ST33HTPH2ExxAHD0	1.38	73.64 (0x49.40)
ST33TPHF20SPI	ST33HTPH20xxAHD7	1.16	74.20 (0x4A.14)
	ST33HTPH20xxAHD1	1.38	74.64 (0x4A.40)
ST33TPHF2EI2C	ST33HTPH2ExxAHC2	1.38	73.65 (0x49.41)
ST33TPHF20I2C	ST33HTPH20xxAHC3	1.38	74.65 (0x4A.41)

1. *Where xx is 28 or 32 depending on the package (TSSOP28 or VQFN32)*

Appendix A Upgrade table

Product name	Commercial part number[1]	FW	TPM library	FW upgrade solution TPM 2.0 revision 1.16	Assets cleared before FW upgrade	New commercial part number[1]	FW upgrade solution TPM 2.0 revision 1.38	Assets cleared before FW upgrade	New commercial part number[1]
ST33TPHF2ESPI	ST33HTPH2ExxAAE6	71.00	1.16	71.16	no	NA	NA	NA	NA
	ST33HTPH2ExxAHA6	71.04	1.16	71.16	no	NA	NA	NA	NA
	ST33HTPH2ExxAHB6	71.12	1.16	71.16	no	NA	NA	NA	NA
	ST33HTPH2ExxAAF1	73.00	1.16	73.20	no	ST33HTPH2ExxAHD6	73.64	yes	ST33HTPH2ExxAHD0
	ST33HTPH2ExxAHB4	73.04	1.16	73.20	no	ST33HTPH2ExxAHD6	73.64	yes	ST33HTPH2ExxAHD0
	ST33HTPH2ExxAHC0	73.08	1.38	NA	NA	NA	73.64	no	ST33HTPH2ExxAHD0
ST33TPHF20SPI	ST33HTPH20xxAAF3	74.00	1.16	74.20	no	ST33HTPH2ExxAHD7	74.64	yes	ST33HTPH20xxAHD1
	NA	74.04	1.16	74.20	no	ST33HTPH2ExxAHD7	74.64	yes	ST33HTPH20xxAHD1
	ST33HTPH20xxAHC1	74.08	1.38	NA	NA	NA	74.64	no	ST33HTPH20xxAHD1
	ST33HTPH20xxAHC9	74.16	1.38	NA	NA	NA	74.64	no	ST33HTPH20xxAHD1
ST33TPHF2EI2C	ST33HTPH2ExxAHB8	73.05	1.16	73.21	no	NA	73.65	yes	NA
	ST33HTPH2ExxAHC2	73.09	1.38	NA	NA	NA	73.65	no	ST33HTPH2ExxAHC2
ST33TPHF20I2C	ST33HTPH20xxAHB9	74.05	1.16	74.21	no	NA	74.65	yes	NA
	ST33HTPH20xxAHC3	74.09	1.38	NA	NA	NA	74.65	no	ST33HTPH20xxAHC3

1. *Where xx is 28 or 32 depending on the package (TSSOP28 or VQFN32)*

Appendix B Acronyms and definitions

The following table contains a list of common acronyms/terms and their meanings.

Table 5. Glossary

Term	Definition
API	Application programming interface
ECDSA	Elliptic curve digital signature algorithm
FW	Firmware
I²C	Inter-integrated circuit
NA	Not applicable
SPI	Serial peripheral interface
TCG	Trusted Computing Group
TPM	Trusted Platform Module

Appendix C Reference documents

The following materials are to be used in conjunction with or are referenced by this document.

Document reference	Document title
[DB2868]	Flash-memory-based TPM 2.0 device with an SPI interface – ST33TPHF20SPI data brief
[DB2716]	Flash-memory-based device combining TPM 1.2 and TPM 2.0 with an SPI interface – ST33TPHF2ESPI data brief
[DB3671]	Flash-memory based TPM 2.0 device with an I²C interface – ST33TPHF20I2C data brief
[DB3670]	Flash-memory based device combining TPM 1.2 and TPM 2.0 with an I²C interface – ST33TPHF2EI2C data brief
[TPM 2.0 r138]	TPM Library, Part 1, Part 2, Part 3, Part 4, Family 2.0, rev 1.38, TCG
[TPM 2.0 r116]	TPM Library, Part 1, Part 2, Part 3, Part 4, Family 2.0, rev 1.16, TCG

Revision history

Table 6. **Document revision history**

Date	Version	Changes
19-Nov-2019	1	Initial release.
15-May-2020	2	Updated Section Appendix A Upgrade table (ST33HTPH20I2C product name instead of ST33HTPH20SPI for ST33HTPH20xxAHC3 commercial part number).

Contents

List of tables