CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

SBA
Research

東京工業大学
Tokyo Institute of Technology

COMET

Competence Centers for Excellent Technologies

On the Usability of Authenticity Checks for Hardware Security Tokens

Katharina Pfeffer, Alexandra Mai, Adrian Dabrowski, Matthias Gusenbauer, Philipp Schindler, Edgar Weippl, Michael Franz, Katharina Krombholz

bmvit Bundesministerium für Verkehr, Innovation und Technologie

bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft

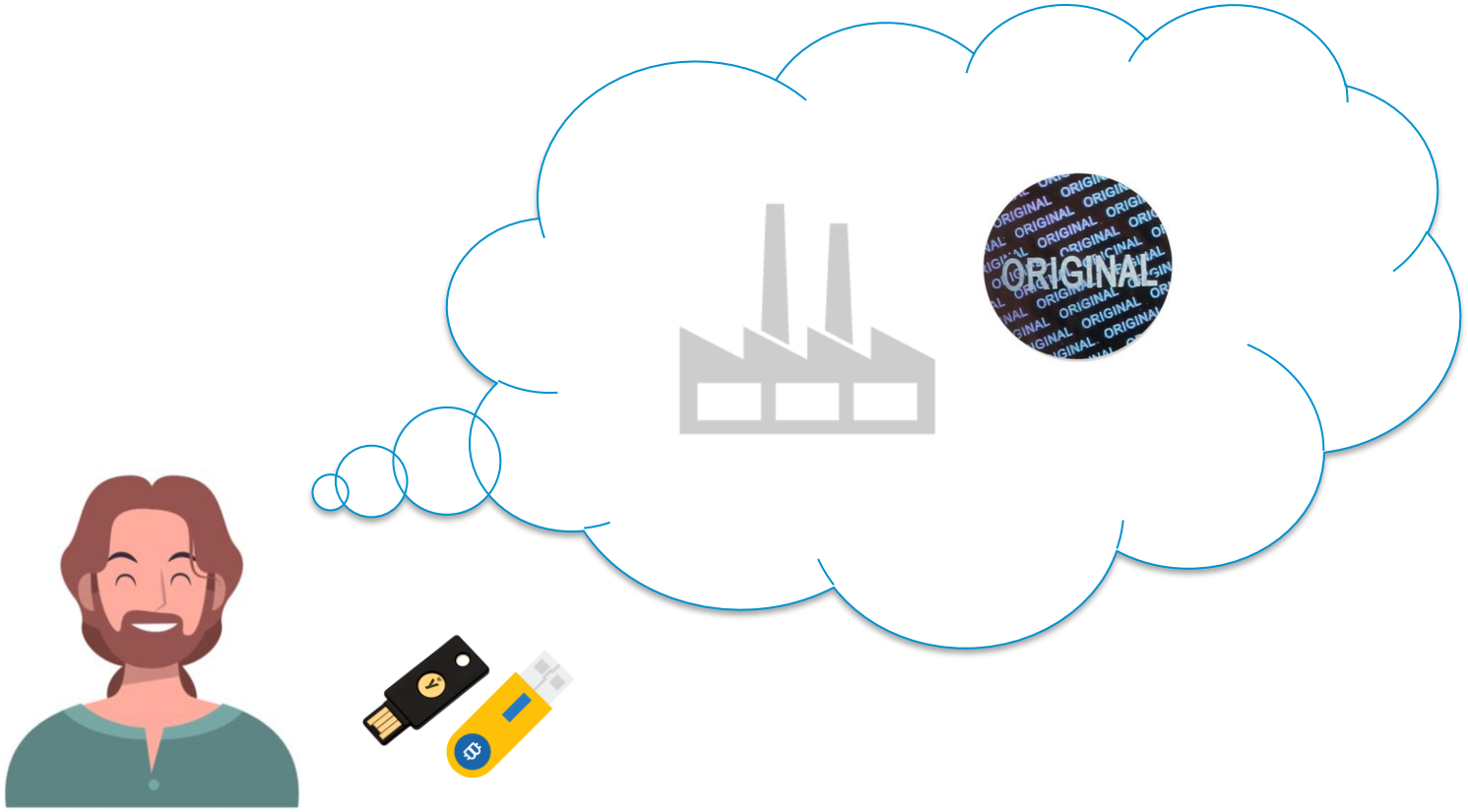
FFG

wirtschaftsagentur wien Ein Fonds der Stadt Wien

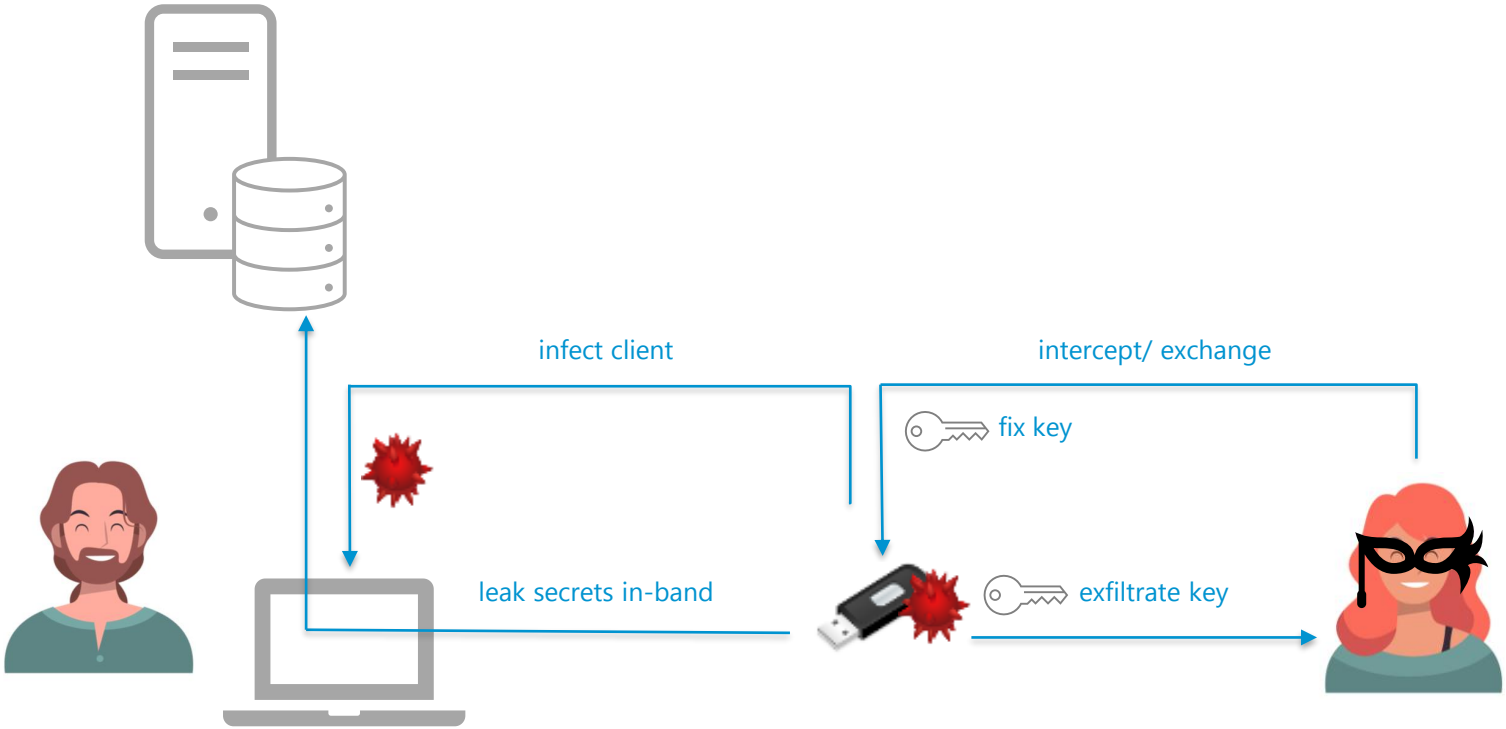
FWF

Christian Doppler Forschungsgesellschaft

netidee powerful innovations


ORIGINAL

Attack Vectors



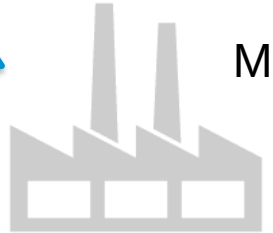
Challenge

Attackers

HST
Authenticity
Checks

End-users

Manufacturers



Research Questions

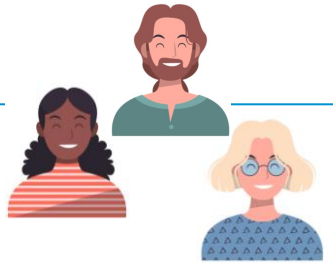
- How **effective** are currently deployed authenticity checks of HSTs in defending against possible attacks?
- How do **users perceive and use** the provided authenticity checks?
- Which (combination of) authenticity checks can **maximize security and usability?**

Methodology



Market Review

Cognitive Walkthroughs → Evaluation Framework



User Study

Discussion Rounds (*N=12*) → Survey (*N=194*)

Market Review Findings

Effectiveness (market review)

○ no prevention
● strong protection
◐ complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✔ potentially used

			Hardware implants	Token replication	IC modification	Firmware modification	USB exploit	Token pre-initialization	Timing side-channels	Bus snooping	IC microprobing	Fault injection
			Attack Vectors									
			Hardware			Software		Secret Extraction				
Attestation / Countermeasure	Pack.	Tamper-evident	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
		Holographic sticker	○	○	○	○	○	○	○	○	○	○
	Hardware	Single-piece cast	●	◐	◐	○	○	○	○	◐	◐	○
		Openable device	◐	◐	○	○	○	○	○	○	○	○
		Secure element (co-processor)	○	●	●	○	○	○	●	◐	●	●
		Secure CPU	◐	●	●	○	○	○	●	●	●	●
	Software	Local firmware attestation	○	○	○	●	○	○	○	○	○	○
		Remote firmware attestation	○	◐	○	●	○	○	○	○	○	○
		Key attestation	○	●	○	◐	○	○	○	○	○	○
		Manual firmware load	○	◐	○	●	○	◐	◐	◐	◐	◐

● fulfilled/implemented/included
◑ sometimes ○ not fullfilled
– not applicable ? undisclosed

		Ledger Nano S	Ledger Blue	Trezor One	Trezor Model T	Keepkey	YubiKey 5	YubiKey 4 Neo	YubiKey 4	Yubico Sec. Key
Pack.	Tamper-evident	○	○	●	○	○	●	◑[1]	◑[1]	◑[1]
	Holographic sticker	○	○	●	●	●	○	◑[1]	◑[1]	◑[1]
Hardware	Single-piece cast	–[2]	–[2]	○	○	○	●	●	●	●
	Openable device	●	●	○	○	○	–[2]	–[2]	–[2]	–[2]
	Secure CPU	○	○	○	○	○	●	○	○	○
	Secure element (co-processor)	●	●	○	○	○	○	●	●	●
Software	Local firmware attestation	●	●	●	●	●	?	?	?	?
	Remote firmware attestation	●	●	○	○	○	○	○	○	○
	Key attestation	●	●	○	○	○	●	●	●	○
	Manual firmware load	○	○	●	●	○	○	○	○	○

[1] Packaging changed multiple times in recent years. [2] Mutually exclusive.

Market Review Findings

Effectiveness (market review)

○ no prevention
● strong protection
◐ complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✔ potentially used

			Hardware implants	Token replication	IC modification	Firmware modification	USB exploit	Token pre-initialization	Timing side-channels	Bus snooping	IC microprobing	Fault injection
			Attack Vectors									
			Hardware			Software			Secret Extraction			
Attestation / Countermeasure	Pack.	Tamper-evident	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
		Holographic sticker	○	○	○	○	○	○	○	○	○	○
	Hardware	Single-piece cast	●	◐	◐	○	○	○	○	◐	◐	○
		Openable device	◐	◐	○	○	○	○	○	○	○	○
		Secure element (co-processor)	○	●	●	○	○	○	●	◐	●	●
		Secure CPU	◐	●	●	○	○	○	●	●	●	●
	Software	Local firmware attestation	○	○	○	●	○	○	○	○	○	○
		Remote firmware attestation	○	◐	○	●	○	○	○	○	○	○
		Key attestation	○	●	○	◐	○	○	○	○	○	○
		Manual firmware load	○	◐	○	●	○	◐	◐	◐	◐	◐

● fulfilled/implemented/included
◑ sometimes ○ not fullfilled
– not applicable ? undisclosed

		Ledger Nano S	Ledger Blue	Trezor One	Trezor Model T	Keepkey	YubiKey 5	YubiKey 4 Neo	YubiKey 4	Yubico Sec. Key
Pack.	Tamper-evident	○	○	●	○	○	●	◑[1]	◑[1]	◑[1]
	Holographic sticker	○	○	●	●	●	○	◑[1]	◑[1]	◑[1]
Hardware	Single-piece cast	–[2]	–[2]	○	○	○	●	●	●	●
	Openable device	●	●	○	○	○	–[2]	–[2]	–[2]	–[2]
	Secure CPU	○	○	○	○	○	●	○	○	○
	Secure element (co-processor)	●	●	○	○	○	○	●	●	●
Software	Local firmware attestation	●	●	●	●	●	?	?	?	?
	Remote firmware attestation	●	●	○	○	○	○	○	○	○
	Key attestation	●	●	○	○	○	●	●	●	○
	Manual firmware load	○	○	●	●	○	○	○	○	○

[1] Packaging changed multiple times in recent years. [2] Mutually exclusive.

Market Review Findings

Effectiveness (market review)
○ no prevention
● strong protection
◐ complicates attack/decreases usefulness

Attack Vector Usage in Scenarios
✔ potentially used

			Hardware implants	Token replication	IC modification	Firmware modification	USB exploit	Token pre-initialization	Timing side-channels	Bus snooping	IC microprobing	Fault injection
			Attack Vectors									
			Hardware			Software			Secret Extraction			
Attestation / Countermeasure	Pack.	Tamper-evident	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
		Holographic sticker	○	○	○	○	○	○	○	○	○	○
	Hardware	Single-piece cast	●	◐	◐	○	○	○	○	◐	◐	○
		Openable device	◐	◐	○	○	○	○	○	○	○	○
		Secure element (co-processor)	○	●	●	○	○	○	●	◐	●	●
		Secure CPU	◐	●	●	○	○	○	●	●	●	●
	Software	Local firmware attestation	○	○	○	●	○	○	○	○	○	○
		Remote firmware attestation	○	◐	○	●	○	○	○	○	○	○
		Key attestation	○	●	○	◐	○	○	○	○	○	○
		Manual firmware load	○	◐	○	●	○	◐	◐	◐	◐	◐

● fulfilled/implemented/included
◑ sometimes ○ not fullfilled
– not applicable ? undisclosed

		Ledger Nano S	Ledger Blue	Trezor One	Trezor Model T	Keepkey	YubiKey 5	YubiKey 4 Neo	YubiKey 4	Yubico Sec. Key
Pack.	Tamper-evident	○	○	●	○	○	●	◑[1]	◑[1]	◑[1]
	Holographic sticker	○	○	●	●	●	○	◑[1]	◑[1]	◑[1]
Hardware	Single-piece cast	–[2]	–[2]	○	○	○	●	●	●	●
	Openable device	●	●	○	○	○	–[2]	–[2]	–[2]	–[2]
	Secure CPU	○	○	○	○	○	●	○	○	○
	Secure element (co-processor)	●	●	○	○	○	○	●	●	●
Software	Local firmware attestation	●	●	●	●	●	?	?	?	?
	Remote firmware attestation	●	●	○	○	○	○	○	○	○
	Key attestation	●	●	○	○	○	●	●	●	○
	Manual firmware load	○	○	●	●	○	○	○	○	○

[1] Packaging changed multiple times in recent years. [2] Mutually exclusive.

Market Review Findings

Effectiveness (market review)
○ no prevention
● strong protection
◐ complicates attack/decreases usefulness

Attack Vector Usage in Scenarios
✔ potentially used

			Hardware implants	Token replication	IC modification	Firmware modification	USB exploit	Token pre-initialization	Timing side-channels	Bus snooping	IC microprobing	Fault injection
			Attack Vectors									
			Hardware			Software			Secret Extraction			
Attestation / Countermeasure	Pack.	Tamper-evident	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
		Holographic sticker	○	○	○	○	○	○	○	○	○	○
	Hardware	Single-piece cast	●	◐	◐	○	○	○	○	◐	◐	○
		Openable device	◐	◐	○	○	○	○	○	○	○	○
		Secure element (co-processor)	○	●	●	○	○	○	●	◐	●	●
		Secure CPU	◐	●	●	○	○	○	●	●	●	●
	Software	Local firmware attestation	○	○	○	●	○	○	○	○	○	○
		Remote firmware attestation	○	◐	○	●	○	○	○	○	○	○
		Key attestation	○	●	○	◐	○	○	○	○	○	○
		Manual firmware load	○	◐	○	●	○	◐	◐	◐	◐	◐

● fulfilled/implemented/included
◑ sometimes ○ not fullfilled
– not applicable ? undisclosed

		Ledger Nano S	Ledger Blue	Trezor One	Trezor Model T	Keepkey	YubiKey 5	YubiKey 4 Neo	YubiKey 4	Yubico Sec. Key
Pack.	Tamper-evident	○	○	●	○	○	●	◑[1]	◑[1]	◑[1]
	Holographic sticker	○	○	●	●	●	○	◑[1]	◑[1]	◑[1]
Hardware	Single-piece cast	–[2]	–[2]	○	○	○	●	●	●	●
	Openable device	●	●	○	○	○	–[2]	–[2]	–[2]	–[2]
	Secure CPU	○	○	○	○	○	●	○	○	○
	Secure element (co-processor)	●	●	○	○	○	○	●	●	●
Software	Local firmware attestation	●	●	●	●	●	?	?	?	?
	Remote firmware attestation	●	●	○	○	○	○	○	○	○
	Key attestation	●	●	○	○	○	●	●	●	○
	Manual firmware load	○	○	●	●	○	○	○	○	○

[1] Packaging changed multiple times in recent years. [2] Mutually exclusive.

Market Review Findings

Effectiveness (market review)

○ no prevention
● strong protection
◐ complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✔ potentially used

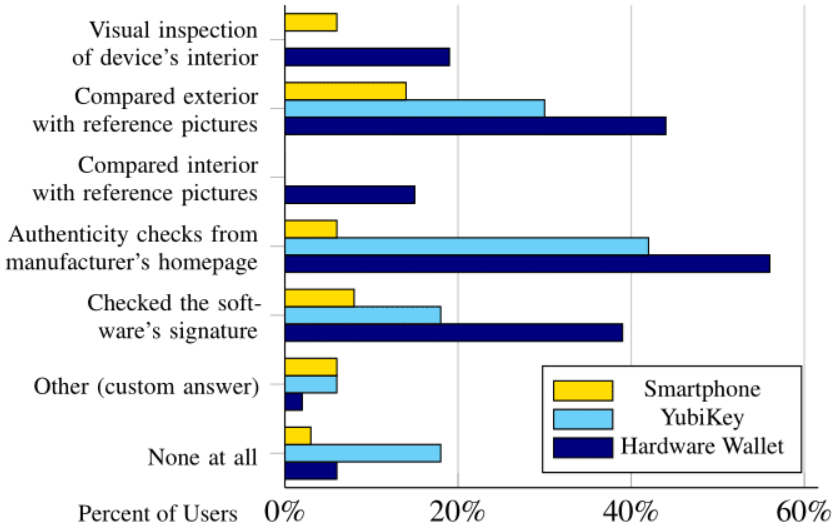
			Hardware implants	Token replication	IC modification	Firmware modification	USB exploit	Token pre-initialization	Timing side-channels	Bus snooping	IC microprobing	Fault injection
			Attack Vectors									
			Hardware			Software			Secret Extraction			
Attestation / Countermeasure	Pack.	Tamper-evident	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
		Holographic sticker	○	○	○	○	○	○	○	○	○	○
	Hardware	Single-piece cast	●	◐	◐	○	○	○	○	◐	◐	○
		Openable device	◐	◐	○	○	○	○	○	○	○	○
		Secure element (co-processor)	○	●	●	○	○	○	●	◐	●	●
		Secure CPU	◐	●	●	○	○	○	●	●	●	●
	Software	Local firmware attestation	○	○	○	●	○	○	○	○	○	○
		Remote firmware attestation	○	◐	○	●	○	○	○	○	○	○
		Key attestation	○	●	○	◐	○	○	○	○	○	○
		Manual firmware load	○	◐	○	●	○	◐	◐	◐	◐	◐

● fulfilled/implemented/included
◑ sometimes ○ not fullfilled
– not applicable ? undisclosed

		Ledger Nano S	Ledger Blue	Trezor One	Trezor Model T	Keepkey	YubiKey 5	YubiKey 4 Neo	YubiKey 4	Yubico Sec. Key
Pack.	Tamper-evident	○	○	●	○	○	●	◑[1]	◑[1]	◑[1]
	Holographic sticker	○	○	●	●	●	○	◑[1]	◑[1]	◑[1]
Hardware	Single-piece cast	–[2]	–[2]	○	○	○	●	●	●	●
	Openable device	●	●	○	○	○	–[2]	–[2]	–[2]	–[2]
	Secure CPU	○	○	○	○	○	●	○	○	○
	Secure element (co-processor)	●	●	○	○	○	○	●	●	●
Software	Local firmware attestation	●	●	●	●	●	?	?	?	?
	Remote firmware attestation	●	●	○	○	○	○	○	○	○
	Key attestation	●	●	○	○	○	●	●	●	○
	Manual firmware load	○	○	●	●	○	○	○	○	○

[1] Packaging changed multiple times in recent years. [2] Mutually exclusive.

User Study Findings



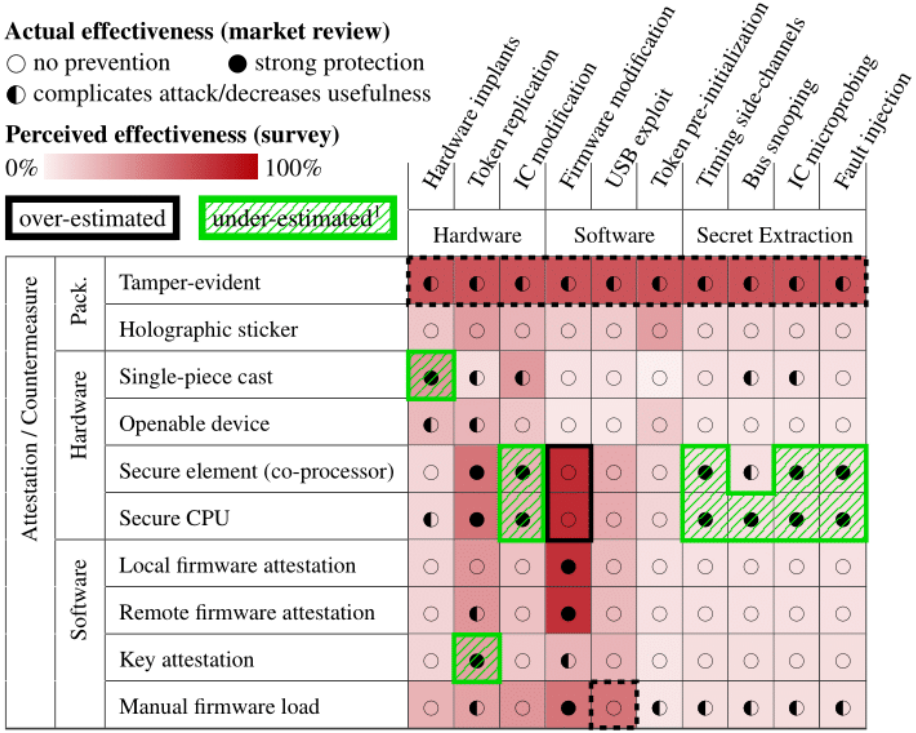
			$\mathcal{H}$	$\mathcal{Y}$	$\mathcal{S}$
Genuine		Yes	95%	82%	93%
		No	0%	0%	3%
		I don't know	5%	17%	5%
Trust Factors	Packaging	not damaged/opened	74%	65%	77%
		vendors name/logo displayed	45%	56%	75%
		high quality	47%	33%	64%
		holographic sticker	33%	31%	34%
	Product	not damaged	65%	70%	79%
		has not been put into operation	40%	12%	36%
		looked genuine	66%	73%	83%
	Trusted	manufacturer	73%	61%	61%
		other people's opinion	63%	68%	50%

Groups: Hardware Wallet ($\mathcal{H}$), YubiKey ($\mathcal{Y}$), and Smartphone users ($\mathcal{S}$). For the trust factors, multiple answers were possible.

Authenticity checks are only carried out by a **fraction of users**

Users' trust is highly influenced by the **packaging**

Perceived vs. Actual Effectiveness



[1] Benefits need to be better explained to customers.

Many **users perceive** the **effectiveness** of deployed attestation methods **incorrectly!**

Perceived vs. Actual Effectiveness

- Gaps between perceived and actual efficiency
  - Reason: **Lack of information and transparency**
  - Users **cannot make informed trust decisions**
- Manufacturers engage in **security theater:**
  - creating a false sense of security

Solution

- Solve current technical and usability issues by a combination of:
  - Secure CPUs/elements
  - Remote firmware attestation
  - User-centered design
    - Transparent authenticity checks
    - Security labels
  - Collaborative protocols (currently not implemented)

COMET

Competence Centers for
Excellent Technologies

Katharina Pfeffer

SBA Research GmbH

https://www.sba-research.org/

kpfeffer@sba-research.org