On the Usability of Authenticity Checks for Hardware Security Tokens

Alexandra Mai and Katharina Pfeffer

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
SBA Research

Problem & Motivation

Hardware security tokens (e.g., hardware wallets, Yubikeys) help users to keep stored secrets secure. However, recently reported attacks suggest that users cannot take the security guarantees of their devices for granted – even despite widely deployed authenticity checks.

Evaluate the effectiveness and usability of authenticity checks, we present (i) the first comprehensive market review analyzing authenticity checks of popular hardware security token and (ii) a large scale survey investigating user perceptions and usage of these checks.

Hardware Security Tokens

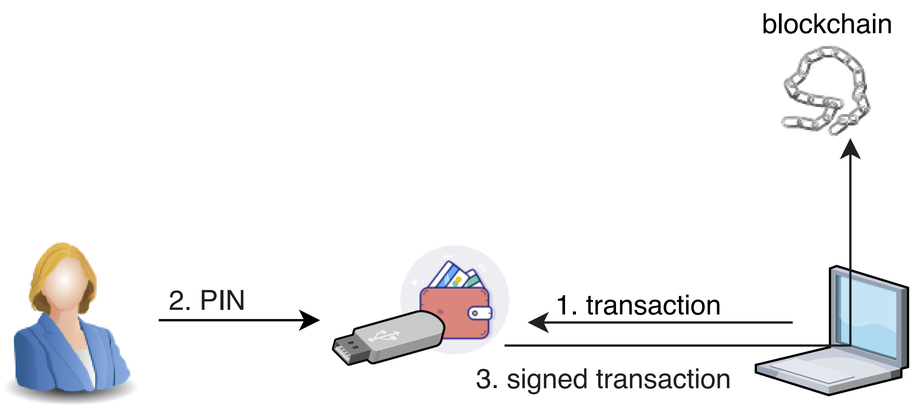

Figure 1: Simplified Hardware Wallet Transaction Model

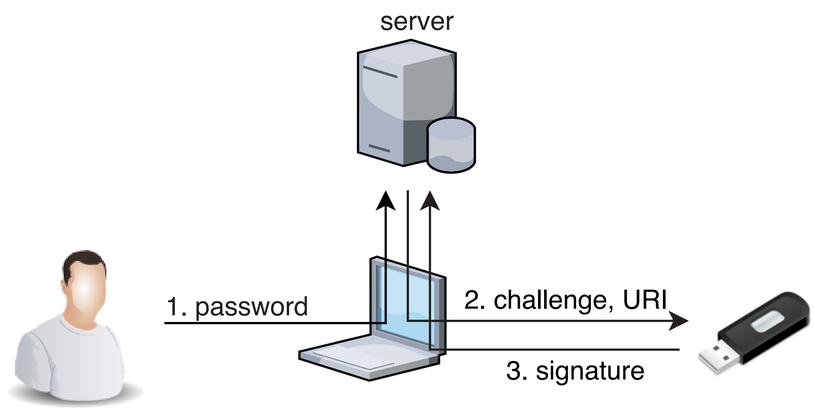

Figure 2: Simplified U2F Authentication Model

Market Review

- Reviewed tokens:
  - 4 YubiKey models
  - 5 hardware wallets
- Methodology: cognitive walkthroughs

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

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

Table 1: Evaluation Framework: Mapping of Authenticity Checks to Attack Vectors

User Survey

- 2 discussion rounds with:
  - 9 HW security token users
  - 3 smartphone users
- Online questionnaire
  - 194 participants
  - 27–30 open/closed questions
  - 3 user groups: HW-Wallet, YubiKey, Smartphone

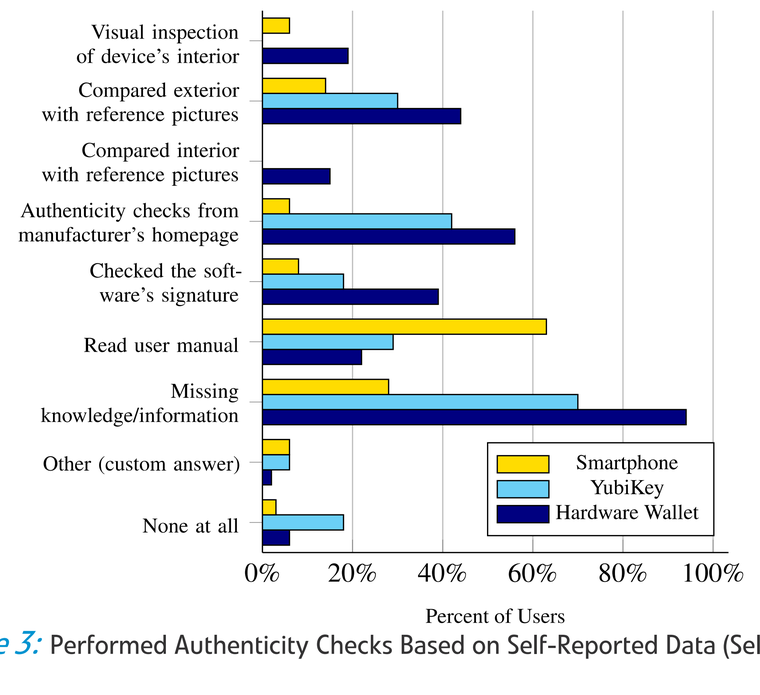

Figure 3: Performed Authenticity Checks Based on Self-Reported Data (Selection)

Conclusion

- Currently deployed authenticity checks—even in best-case implementations—are not sufficient to defeat all distribution attacks.
- Users incorrectly assess the existence and the security guarantees of many authenticity checks due to a lack of information and visibility.
- Recommendation: A combination of (i) secure CPUs or elements, (ii) remote firmware attestation, (iii) a recently proposed method for collaborative and verifiable key generation, and (iv) a user-friendly transparent design.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.