

SBA Research





東京工業大学
Tokyo Institute of Technology



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







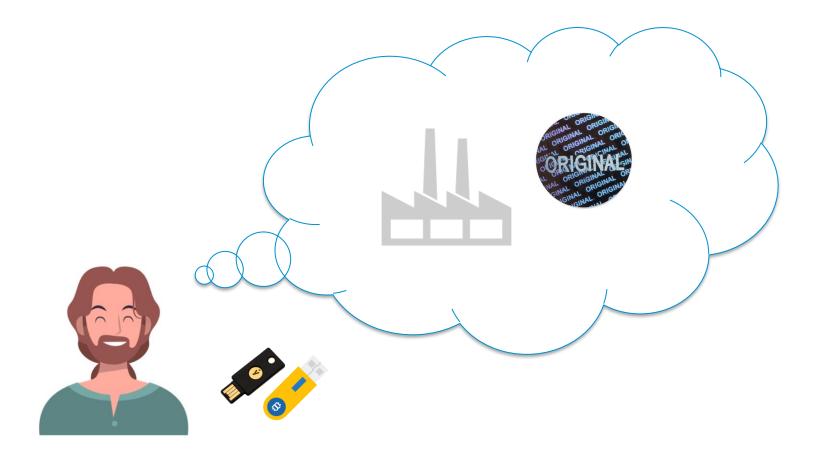
* Ein Fonds der Stadt Wien



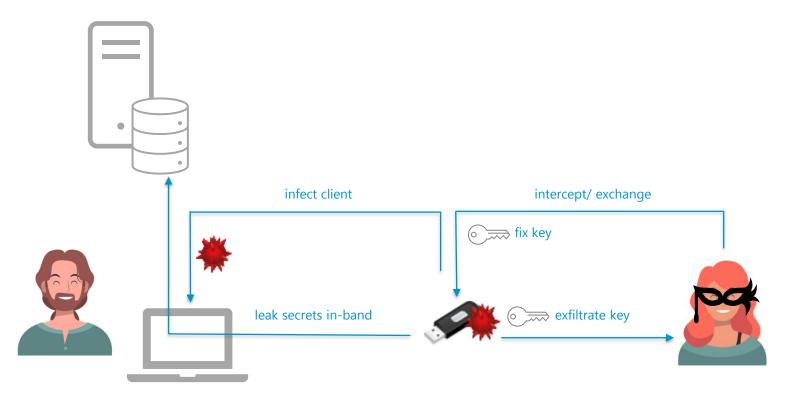
Christian Dopple Forschungsgesellschaf

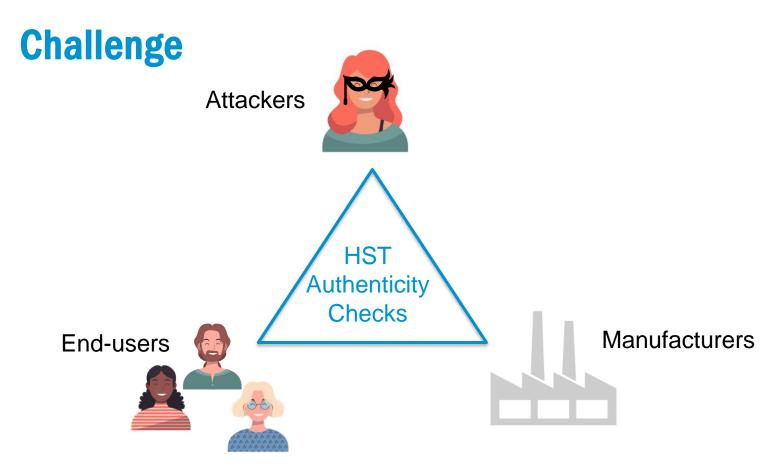


2



Attack Vectors

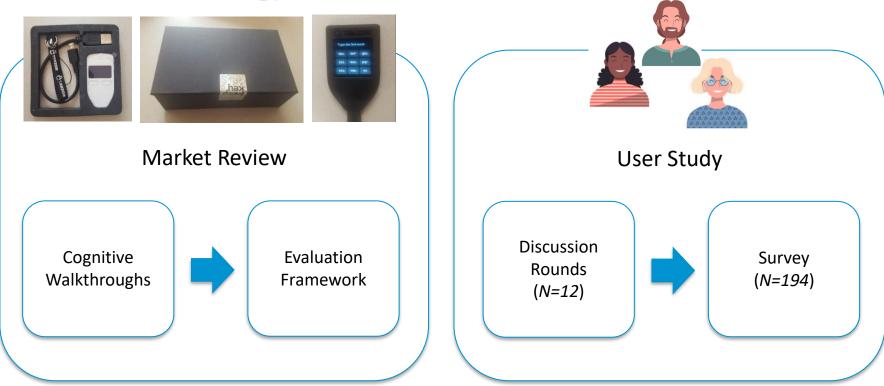




Research Questions

- 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



Token Pplication

L'undification

Loven Dechning

Bus shooping

Lanic and a start

Fault injection

Finnear Production

Attack Vectors

Effectiveness (market review)

- \bigcirc no prevention
- strong protection
- Harding are inplants € complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✓ potentially used

			Ha	ardwa	are	S	oftwa	re	Secret Extraction				
ure	Pack.	Tamper-evident	•	•	•	Ð	•	O	•	•	•	Ð	
Attestation / Countermeasure	Pa	Holographic sticker	0	0	0	0	0	0	0	0	0	0	
unter	are	Single-piece cast	•	0	0	0	0	0	0	•	•	0	
/Co	Hardware	Openable device	•	•	0	0	0	0	0	0	0	0	
ation	H	Secure element (co-processor)	0	•	•	0	0	0	•	•	•	•	
Attest		Secure CPU	•	•	•	0	0	0	•	•	•	•	
	are	Local firmware attestation	0	0	0	•	0	0	0	0	0	0	
	Software	Remote firmware attestation	0	•	$^{\circ}$	•	0	0	0	0	0	0	
		Key attestation	0	•	0	0	0	0	0	0	0	0	
		Manual firmware load	0	0	0	•	0	0	0	0	0	Ð	

- fulfilled/implemented/included • sometimes ○ not fullfilled
- not applicable ? undisclosed

•	fulfilled/implemented/included sometimes O not fullfilled ot applicable ? undisclosed	Ledo-	Leda Nano, C	Tres Blue	Tree of	teen del'	E reference in	Lubit	Lubit Aco	Lubic V	- tose ter
Pack.	Tamper-evident	0	0	•	0	0	•	\mathbf{O}^1	\bullet^1	\bullet^1	
Pa	Holographic sticker	0	0	•	•	•	0	\mathbf{O}^1	\bullet^1	\bullet^1	
	Single-piece cast	_2	_2	0	0	0	•	•	•	•	
Hardware	Openable device	•	•	0	0	0	_2	_2	_2	_2	
Hard	Secure CPU	0	0	0	0	0	•	0	0	0	
	Secure element (co-processor)	•	•	0	0	0	0	•	•	•	
	Local firmware attestation	•	•	•	•	•	?	?	?	?	
Software	Remote firmware attestation	•	•	0	0	0	0	0	0	0	
Soft	Key attestation	•	•	0	0	0	•	•	•	0	
	Manual firmware load	0	0	•	•	0	0	0	0	0	

Loken teplication

Effectiveness (market review)

- \bigcirc no prevention
- strong protection
- Hadua Harding € complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✓ potentially used

	1 5												
				ardwa	are	Se	oftwa	re	Secret Extraction				
ure	Pack.	Tamper-evident	•	•	Ð	•	0	•	Ð	•	•	Ð	
measi	Pa	Holographic sticker	0	0	0	0	0	0	0	0	0	0	
unter	are	Single-piece cast	•	•	Ð	0	0	0	0	•	Ð	0	
Attestation / Countermeasure	Hardware	Openable device	0	0	0	0	0	0	0	0	0	0	
ation		Secure element (co-processor)	0	٠	٠	0	0	0	•	•	•	٠	
Attest		Secure CPU	•	•	•	0	0	0	•	•	•	•	
	are	Local firmware attestation	0	0	0	•	0	0	0	0	0	0	
	Software	Remote firmware attestation	0	•	0	•	0	0	0	0	0	0	
	S	Key attestation	0	•	0	0	0	0	0	0	0	0	
		Manual firmware load	0	•	0	•	0	0	•	•	•	0	

Ach 'plan	IC no.	Funt	USB are modifi	Toten total	Timin Pre-initial	Bus Side chan	IC noping unels	Fault in Obiobino	"Jection"	-	fulfilled/implemented/included
		A	ttack	Vecto	ors	ret E				– ne	ot applicable ? undisclosed
))	are •	•	01twa	•	0	et E	•	tion O		Pack.	Tamper-evident
)	0	0	0	0	0	0	0	0		Pa	Holographic sticker
)	Ð	0	0	0	0	•	Ð	0			Single-piece cast
)	0	0	0	0	0	0	0	0		Hardware	Openable device
)	•	0	0	0	•	0	•	•		Hard	Secure CPU
			-		1		<u> </u>				

Software

Manual firmware load

alfilled/implemented/included ometimes () not fullfilled t applicable ? undisclosed	Ledo.	Leda Nano.s	Tres Blue	Tree, One	teen dode z	Lubit	Lubit	Fubir Neo	Pubje	- ose ter
Tamper-evident	0	0	•	0	0	•	\mathbf{O}^1	$\mathbf{\Phi}^1$	\mathbf{O}^1	
Holographic sticker	0	0	•	•	•	0	\mathbf{O}^1	\mathbf{O}^1	$igodot^1$	
Single-piece cast	_2	_2	0	0	0	•	٠	•	•	
Openable device	•	•	0	0	0	_2	_2	_2	_2	
Secure CPU	0	0	0	0	0	•	0	0	0	
Secure element (co-processor)	•	•	0	0	0	0	•	•	•	
Local firmware attestation	•	•	•	•	•	?	?	?	?	
Remote firmware attestation	•	•	0	0	0	0	0	0	0	
Key attestation	•	•	0	0	0	•	•	•	0	

٠ •

Token teblication

L'undification

Foren Pre-initialization

Busshophig

Lanic and a second

Fault injection

Finner notified

Attack Vectors

Effectiveness (market review)

- \bigcirc no prevention
- strong protection
- Harding are inplants € complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✓ potentially used

•	· potentially used													
			Ha	ardwa	are	So	oftwa	re	Secret Extraction					
ure	Pack.	Tamper-evident	Ð	O	Ð	Ð	●	Ð	Ð	•	Ð	Ð		
Attestation / Countermeasure	Pa	Holographic sticker	\circ	0	0	0	0	0	0	0	0	0		
unter	are	Single-piece cast	•	•	Ð	0	0	0	0	•	Ð	0		
/ C0	Hardware	Openable device	•	0	0	0	0	0	0	0	0	0		
ation	H	Secure element (co-processor)	0	•	•	0	0	0	•	•	•	•		
Attest		Secure CPU	•	•	•	0	0	0	•	•	•	•		
	are	Local firmware attestation	0	0	0	•	0	0	0	0	0	0		
	Software	Remote firmware attestation	0	•	0	•	0	0	0	0	0	0		
	s	Key attestation	0	•	0	•	0	0	0	0	0	0		
		Manual firmware load	0	0	0	•	0	0	•	•	•	Ð		

 fulfilled/imple 	mented/included
sometimes	\bigcirc not fullfilled
 not applicable 	? undisclosed

•	fulfilled/implemented/included sometimes O not fullfilled ot applicable ? undisclosed	Ledo	Ledo Nano S	Tres Blue	The Open	feen Model 2	Fubir	Pubits	Pubit Aco	Pubic A	- cose ter
Pack.	Tamper-evident	0	0	•	0	0	•	\mathbf{O}^1	\mathbf{O}^1	\mathbf{O}^1	
Pa	Holographic sticker	0	0	•	•	•	0	\mathbf{O}^1	\mathbf{O}^1	\mathbf{O}^1	
	Single-piece cast	_2	_2	0	0	0	•	٠	•	•	
ware	Openable device	•	•	0	0	0	_2	_2	_2	_2	
Hardware	Secure CPU	0	0	0	0	0	•	0	0	0	
	Secure element (co-processor)	•	•	0	0	0	0	•	•	•	
	Local firmware attestation	•	•	•	•	•	?	?	?	?	
Software	Remote firmware attestation	•	•	0	0	0	0	0	0	0	
Soft	Key attestation	•	•	0	0	0	•	•	•	0	
	Manual firmware load	0	0	•	•	0	0	0	0	0	

Token tepication

L'undification

Tokon Die hining

Timi -uge side clampels

Bus shooping

TC microsoft

Fault injection

Finnear Production

Attack Vectors

Effectiveness (market review)

- \bigcirc no prevention
- strong protection
- Harding are inplants € complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

✓ potentially used

1 5												
			ardwa	are	Se	oftwa	re	Secret Extraction				
ck.	Tamper-evident	•	•	Ð	Ð	•	Ð	•	•	Ð	Ð	
Pa	Holographic sticker	0	0	0	0	0	0	0	0	0	0	
are	Single-piece cast	•	•	Ð	0	0	0	0	•	0	0	
ardw	Openable device	•	0	0	0	0	0	0	0	0	0	
Ξ	Secure element (co-processor)	0	٠	٠	0	0	0	٠	•	٠	٠	
	Secure CPU	•	•	•	0	0	0	•	•	•	•	
are	Local firmware attestation	0	0	0	٠	0	0	0	0	0	0	
oftw	Remote firmware attestation	0	•	0	•	0	0	0	0	0	0	
	Key attestation	0	•	0	0	0	0	0	0	0	0	
	Manual firmware load	0	•	0	•	0	0	•	•	0	0	
	Software Hardware Pack.	Yord Tamper-evident Holographic sticker Single-piece cast Openable device Secure element (co-processor) Secure CPU Local firmware attestation Remote firmware attestation Key attestation	Yord Tamper-evident • Holographic sticker • Bingle-piece cast • Openable device • Secure element (co-processor) • Secure CPU • Local firmware attestation • Remote firmware attestation • Key attestation •	Yord Tamper-evident ① ① Holographic sticker ○ ○ ○ Single-piece cast ● ○ ○ Openable device ① ○ ○ Secure element (co-processor) ○ ○ Secure CPU ① ● Local firmware attestation ○ ○ Remote firmware attestation ○ ○ Key attestation ○ ●	Yard Hardware Yard Tamper-evident 0 0 0 Holographic sticker 0 0 0 0 Single-piece cast 0 0 0 0 Openable device 0 0 0 0 Secure element (co-processor) 0 0 0 Secure CPU 0 0 0 0 Remote firmware attestation 0 0 0 Key attestation 0 0 0	Yard Tamper-evident 0 0 0 0 Holographic sticker 0 0 0 0 0 Single-piece cast 0 0 0 0 0 0 Openable device 0 0 0 0 0 0 0 Secure element (co-processor) 0 0 0 0 0 0 0 Secure CPU 0 0 0 0 0 0 0 0 Remote firmware attestation 0 0 0 0 0 0 0 Key attestation 0 0 0 0 0 0 0	$\begin{tabular}{ c c c } \hline Hardware interval i$	Hardware Software Yard Tamper-evident Image: Colspan="2">Image: Colspan="2">Colspan="2" Colspan="2" Colspan="2" Colspan="2" Colspan="2" Colspan="2" Colspan="2" Colspan="2" Colspan="2" <th c<="" th=""><th>$\begin{tabular}{ c c c c } \hline Hardware attestation & Hardware & Software & Sector \\ \hline Hallow restricted & 0 &$</th><th></th><th>$\begin{tabular}{ c c c c c } \hline Hardware interval in the set of t$</th></th>	<th>$\begin{tabular}{ c c c c } \hline Hardware attestation & Hardware & Software & Sector \\ \hline Hallow restricted & 0 &$</th> <th></th> <th>$\begin{tabular}{ c c c c c } \hline Hardware interval in the set of t$</th>	$\begin{tabular}{ c c c c } \hline Hardware attestation & Hardware & Software & Sector \\ \hline Hallow restricted & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & $		$\begin{tabular}{ c c c c c } \hline Hardware interval in the set of t$

fulfilled/imple	mented/included	ŝ
sometimes	\bigcirc not fullfilled	A and A and
not applicable	? undisclosed	or of see

•	fulfilled/implemented/included sometimes O not fullfilled ot applicable ? undisclosed	Ledo	Ledo Vano, S	Tres Blue	Tree, one	teen, nodel 2	E reference in	Lubit	Fubix Neo	Pubic 4	- tose ter
Pack.	Tamper-evident	0	0	•	0	0	•	\mathbf{O}^1	\bullet^1	\mathbf{O}^1	
Pa	Holographic sticker	0	0	•	•	•	0	\mathbf{O}^1	\bullet^1	\mathbf{O}^1	
	Single-piece cast	_2	_2	0	0	0	•	•	•	•	
Hardware	Openable device	•	•	0	0	0	_2	_2	_2	_2	
Hard	Secure CPU	0	0	0	0	0	•	0	0	0	
	Secure element (co-processor)	•	•	0	0	0	0	•	•	•	
	Local firmware attestation	٠	٠	٠	٠	•	?	?	?	?	
Software	Remote firmware attestation	•	•	0	0	0	0	0	0	0	
Soft	Key attestation	•	•	0	0	0	•	•	•	0	
	Manual firmware load	0	0	•	•	0	0	0	0	0	

Token teplication

IC modification

Finner notified

Attack Vectors

Loten De Unider

Lanic and a second

Bus shooping

Faultinjetion

Effectiveness (market review)

- \bigcirc no prevention
- strong protection
- Harding are inplants € complicates attack/decreases usefulness

Attack Vector Usage in Scenarios

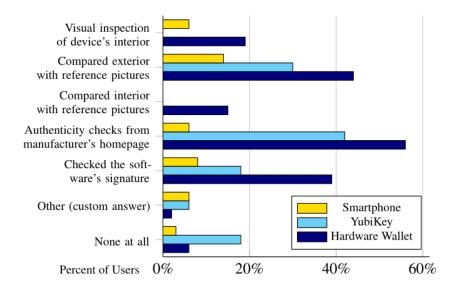
✓ potentially used

· potentially abea													
			Hardware			Software			Secret Extraction				
ure	Pack.	Tamper-evident	•	●	Ð	●	•	•	Ð	0	Ð	O	
meas	Pa	Holographic sticker	0	0	0	0	0	0	0	0	0	0	
untern	Hardware	Single-piece cast	•	0	0	0	0	0	0	0	0	0	
/ C01		Openable device	•	0	0	0	0	0	0	0	0	0	
Attestation / Countermeasure		Secure element (co-processor)	0	•	•	0	0	0	•	0	•	•	
Attest		Secure CPU	•	•	•	0	0	0	•	•	•	•	
	Software	Local firmware attestation	0	0	0	•	0	0	0	0	0	0	
		Remote firmware attestation	0	0	0	٠	0	0	0	0	0	0	
		Key attestation	0	٠	0	•	0	0	0	0	0	0	
		Manual firmware load	0	0	0	•	0	0	0	0	0	Ð	
					-								

•	fulfilled/implemented/included						
0	sometimes	\bigcirc not fullfilled					

● fulfilled/implemented/included ● sometimes ○ not fullfilled - not applicable ? undisclosed							Public A	- cose ter			
Pack.	Tamper-evident	0	0	•	0	0	•	\bullet^1	\bullet^1	\bullet^1	
Pa	Holographic sticker	0	0	•	•	•	0	\bullet^1	\bullet^1	\mathbf{O}^1	
	Single-piece cast	_2	_2	0	0	0	•	•	•	•	
Hardware	Openable device	•	•	0	0	0	_2	_2	_2	_2	
Hard	Secure CPU	0	0	0	0	0	•	0	0	0	
	Secure element (co-processor)	•	•	0	0	0	0	•	•	•	
	Local firmware attestation	•	•	•	•	•	?	?	?	?	
Software	Remote firmware attestation	٠	٠	0	0	0	0	0	0	0	
Soft	Key attestation	٠	٠	0	0	0	•	٠	٠	0	
	Manual firmware load	0	0	•	•	0	0	0	0	0	

User Study Findings



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

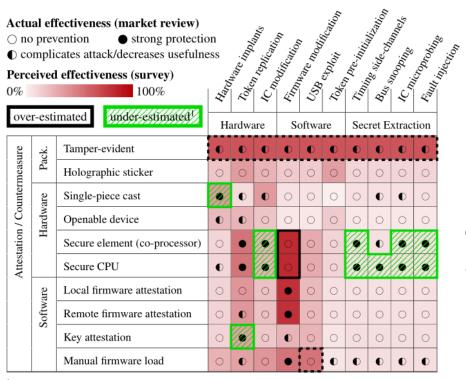
al

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



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

¹ Benefits need to be better explained to customers.

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)





Competence Centers for Excellent Technologies

Katharina Pfeffer

SBA Research GmbH

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

kpfeffer@sba-research.org















