Formal Analysis and Patching of BLE-SC Pairing

Min Shi, Jing Chen, Kun He, Haoran Zhao, Meng Jia, Ruiying Du

Wuhan University, China

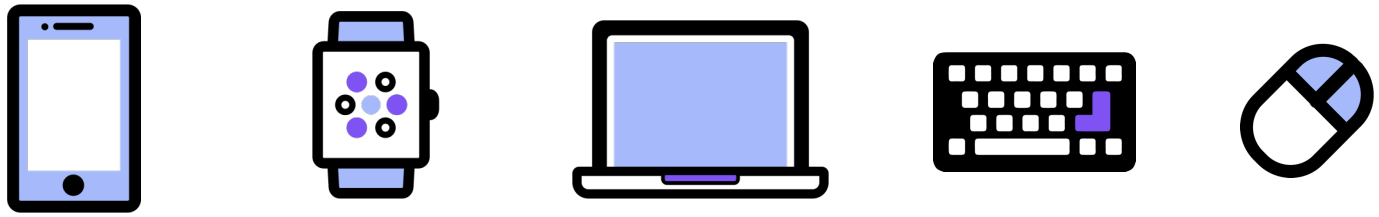
WUHAN
UNIVERSITY

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

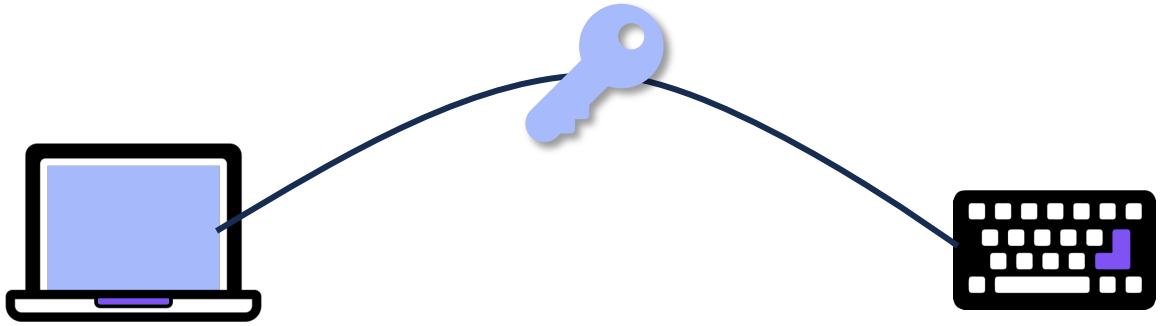
BLE-SC Pairing

Bluetooth Low Energy (BLE)

Connecting devices with minimal energy overhead.



Pairing



BLE Secure Connection (**BLE-SC**) is the latest pairing protocol in BLE.

Motivation

Broken

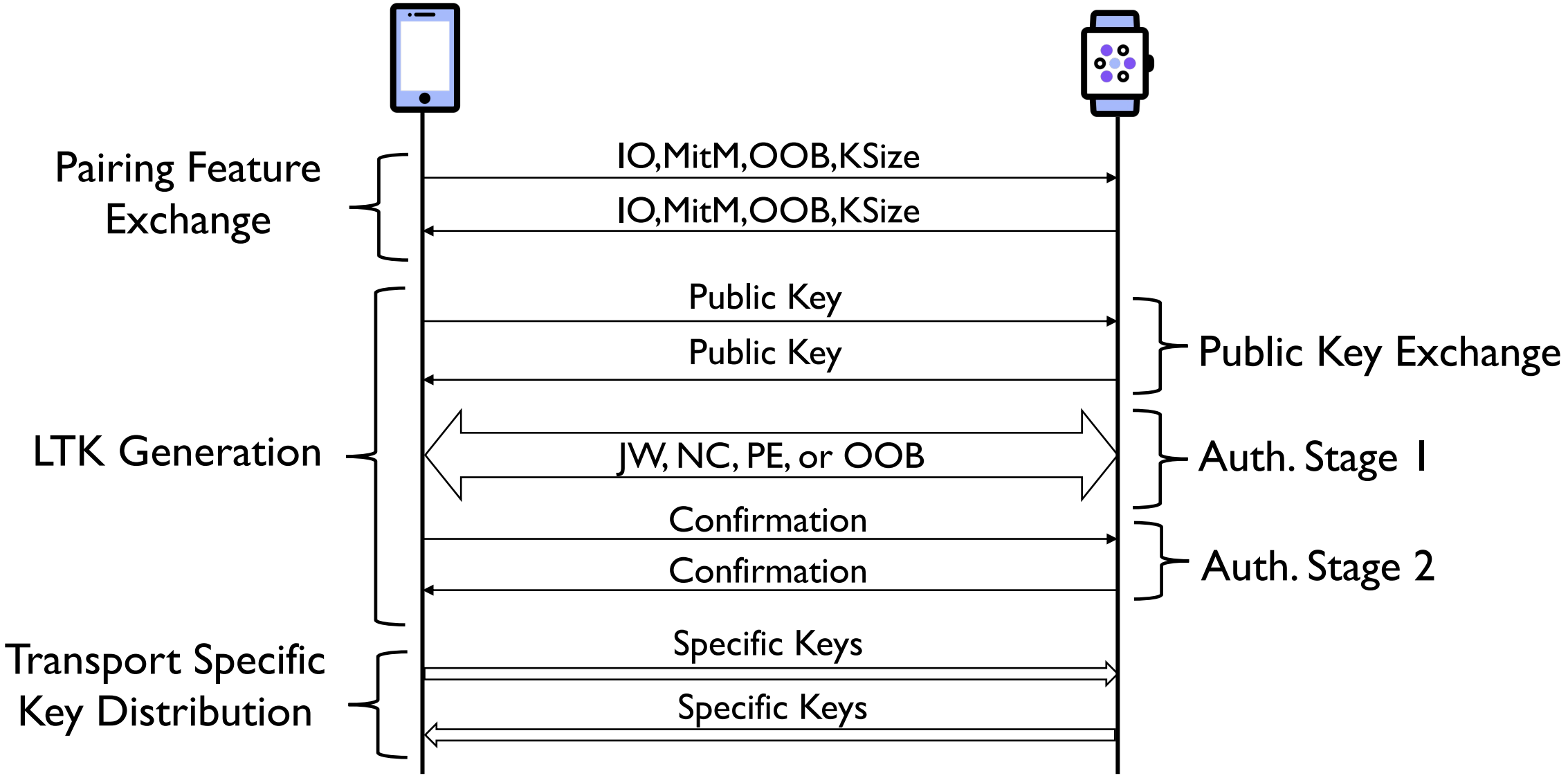
- Tschirschnitz et. al. disclosed the Method Confusion Attack (MCA) .
- Their countermeasures have backward compatibility issue.

Questions

- *How to formally analyze the security of the BLE-SC pairing protocol and disclose the design flaws?*
- *How to fix the found design flaws while maintaining backward compatibility?*

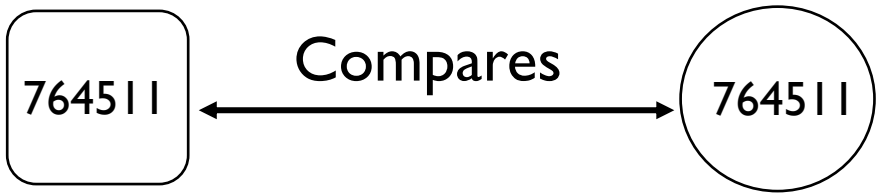
➢ von Tschirschnitz, M., Peuckert, L., Franzen, F., & Grossklags, J. (2021, May). Method confusion attack on bluetooth pairing. In *2021 IEEE symposium on security and privacy (SP)* (pp. 1332-1347). IEEE.

BLE-SC Pairing

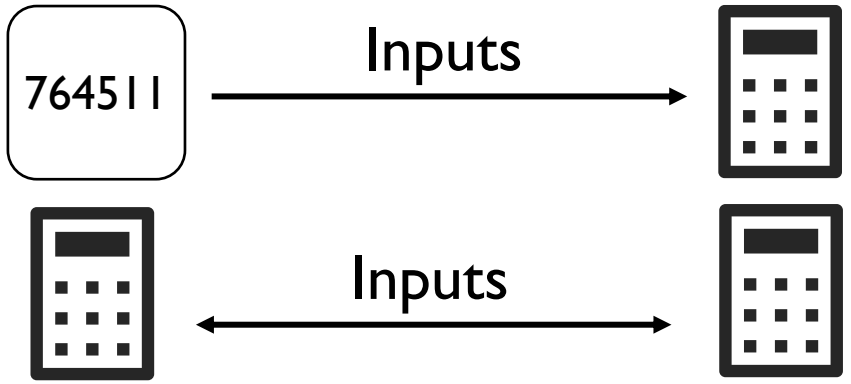


Association Models

Numeric Comparison (NC)



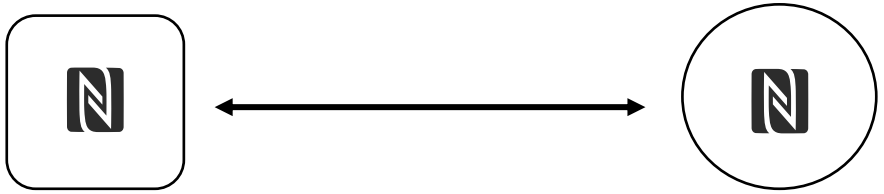
Passkey Entry (PE)



Just Work (JW)

Protocol flows are most like NC,
but do not need user to confirm.
Not Prevent MITM.

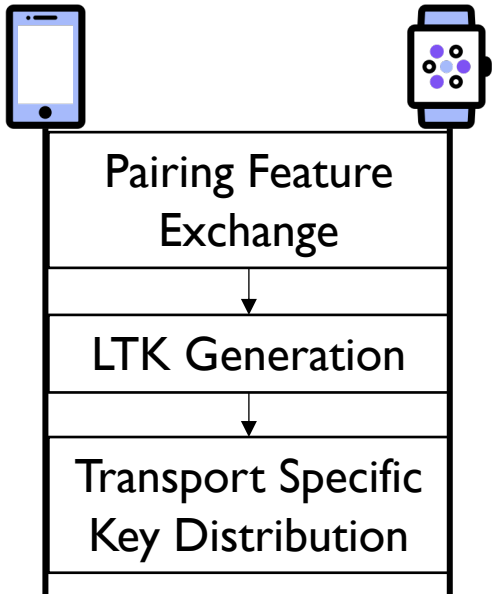
Out Of Band (OOB)

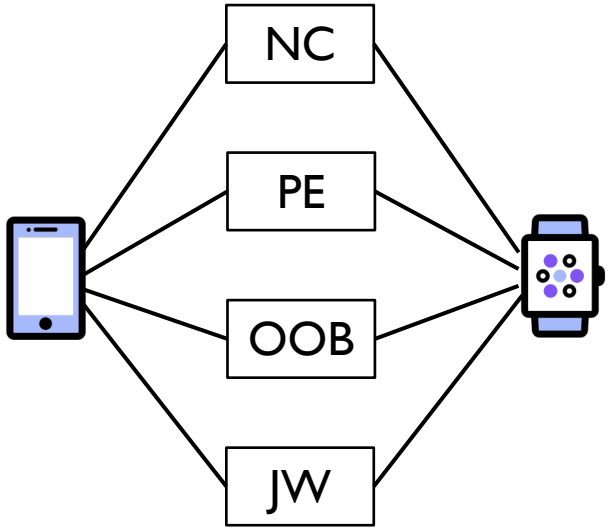


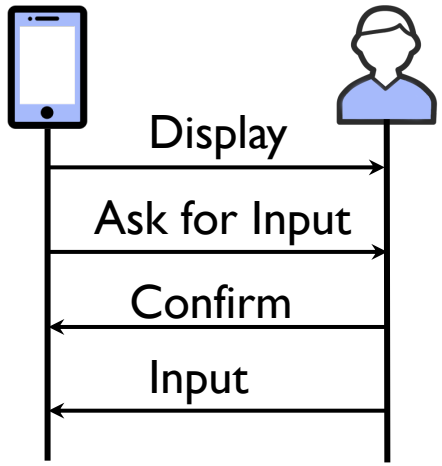
Comprehensive Formal Model

- We use *Tamarin Prover* (symbolic modeling and analysis of security protocols.)
- **Dolev-Yao adversary** with an **additional capability of brute forcing low entropy keys**.

Model Covers:



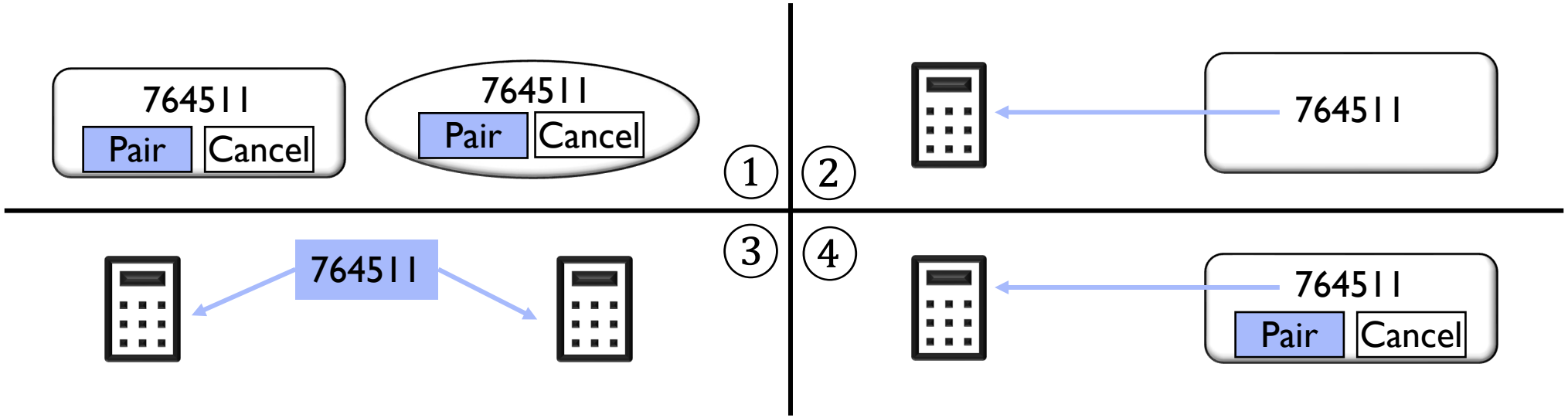




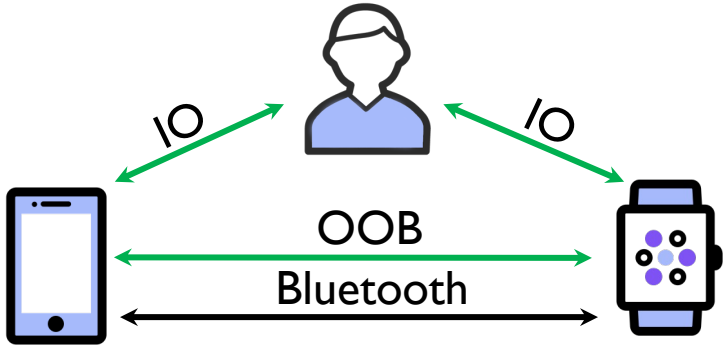
➢ *Meier, S., Schmidt, B., Cremers, C., & Basin, D. (2013). The TAMARIN prover for the symbolic analysis of security protocols. In Computer Aided Verification: 25th International Conference, CAV 2013.*

User & Channel Assumptions

User Assumptions

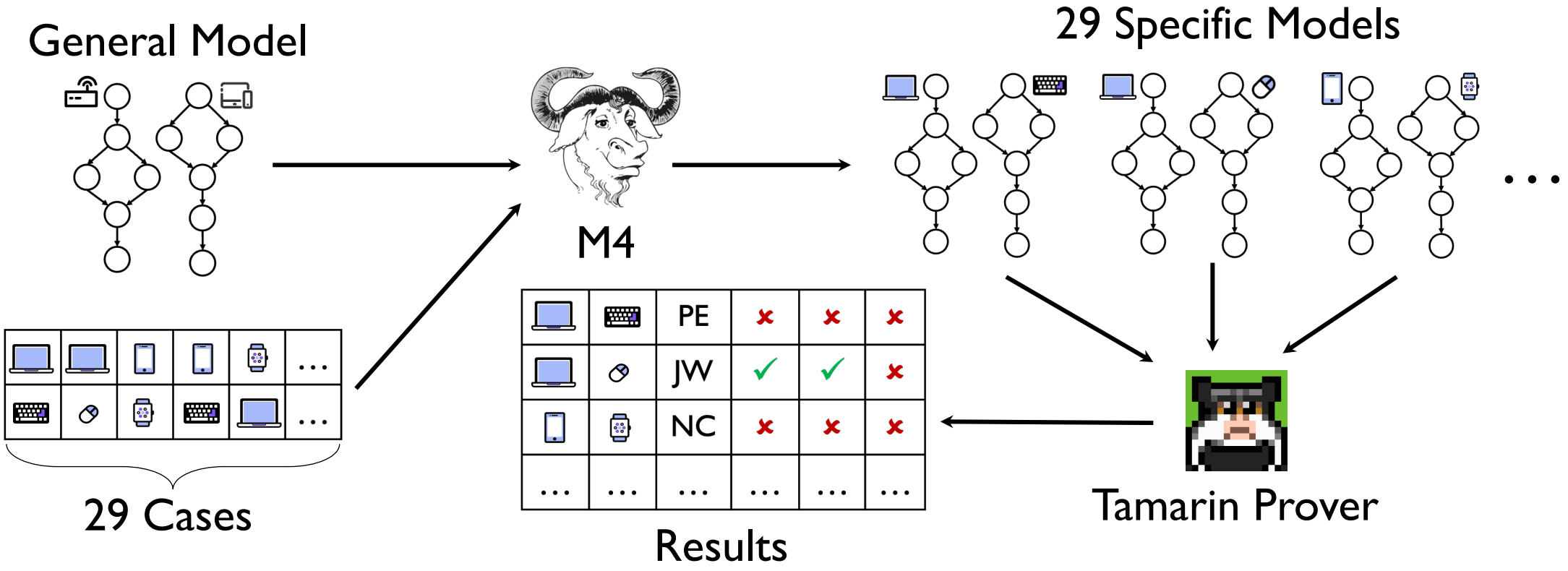


Channel Assumptions



- von Tschirschnitz, M., Peuckert, L., Franzen, F., & Grossklags, J. (2021, May). Method confusion attack on bluetooth pairing. In *2021 IEEE symposium on security and privacy (SP)* (pp. 1332-1347). IEEE.

General-Specific Models



Analysis Results

We verified

- Four authentication properties.
- MitM Protection.
- LTK Confusion Protection.
- Secrecy of Authenticated LTK.

Verification was fully automatic.

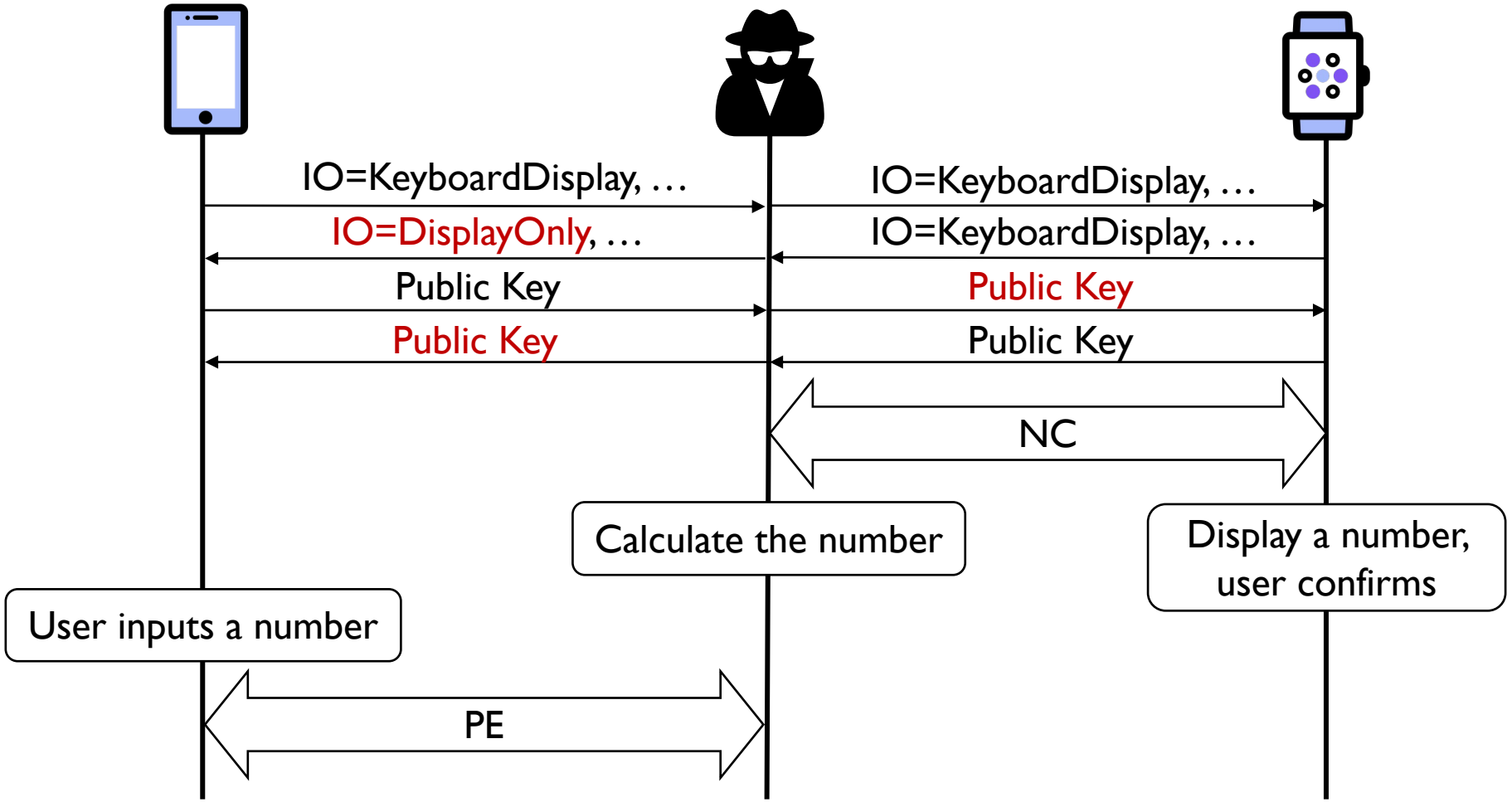
Attacks:

- Confirms two exisiting attacks.
- Discloses a new attack.

No.	Pairing Cases	Exe.	P1	P2	C
1	DisplayYesNo-DisplayYesNo	NC	✓	×	×
2	DisplayYesNo-KeyboardDisplay	NC	×	×	×
3	KeyboardDisplay-KeyboardDisplay	NC	×	×	×
4	KeyboardDisplay-DisplayYesNo	NC	×	×	×
5	DisplayOnly-KeyboardOnly	PE	✓	×	×
6	DisplayOnly-KeyboardDisplay	PE	✓	×	×
7	DisplayYesNo-KeyboardOnly	PE	×	×	×
8	KeyboardOnly-DisplayOnly	PE	✓	×	×
9	KeyboardOnly-DisplayYesNo	PE	×	×	×
10	KeyboardOnly-KeyboardOnly	PE	✓	×	×
11	KeyboardOnly-KeyboardDisplay	PE	×	×	×
12	KeyboardDisplay-DisplayOnly	PE	✓	×	×
13	KeyboardDisplay-KeyboardOnly	PE	×	×	×
14-25	Other Pairs (12)	JW	✓	✓	×
26	No-OOB-No-MITM	JW	✓	✓	×
27	Uni-direction OOB (I→R)	OOB	✓	×	×
28	Uni-direction OOB (I←R)	OOB	✓	×	×
29	Bi-direction OOB (I←→R)	OOB	✓	×	×

- Models & Results: https://github.com/luojiazhishu/BLE-SC-Pairing-Model
- Or Browser Results Only: https://luojiazhishu.github.io/BLE-SC-Pairing-Model/

Method Confusion Attack



- von Tschirschnitz, M., Peuckert, L., Franzen, F., & Grossklags, J. (2021, May). Method confusion attack on bluetooth pairing. In *2021 IEEE symposium on security and privacy (SP)* (pp. 1332-1347). IEEE.

Method Confusion Attack

Affected Cases found *automatedly*

$IOCap_R$	$IOCap_I$		
	DisplayYesNo	KeyboardOnly	DisplayKeyboard
DisplayYesNo	N/A	MCA-PN	MCA-PN
KeyboardOnly	MCA-NP	N/A	MCA-NP
DisplayKeyboard	MCA-NP	MCA-PN	MCA-NP*

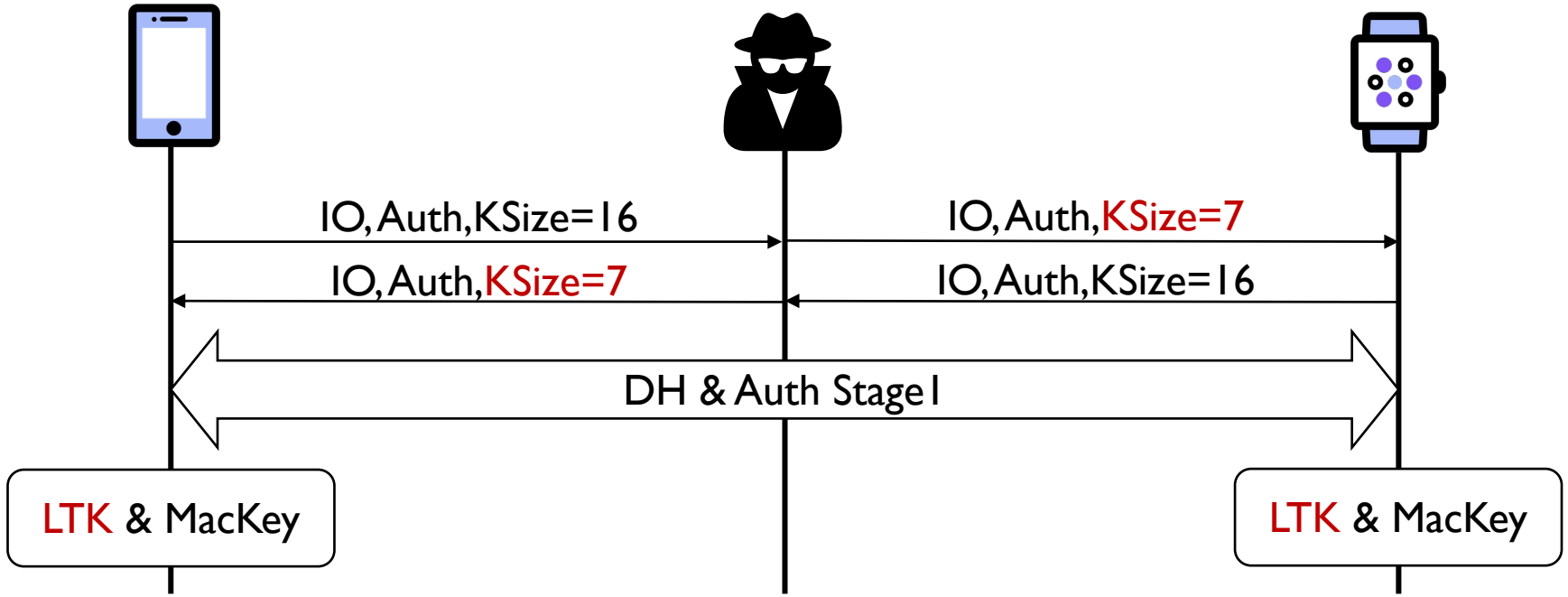
MCA-PN: Initiator PE, Responder NC.
MCA-NP: Initiator NC, Responder PE.
**:There should be MCA-PN & MCA-NP, but Tamarin only give one Counterexample.*

Countermeasures

- Enforcing Pairing Method
- User Interface Design Hotfix
- Authenticating Association Model

"Currently **there is no fix** available that would not massively affect backwards compatibility to older Bluetooth devices."

Key Negotiation Downgrade Attack

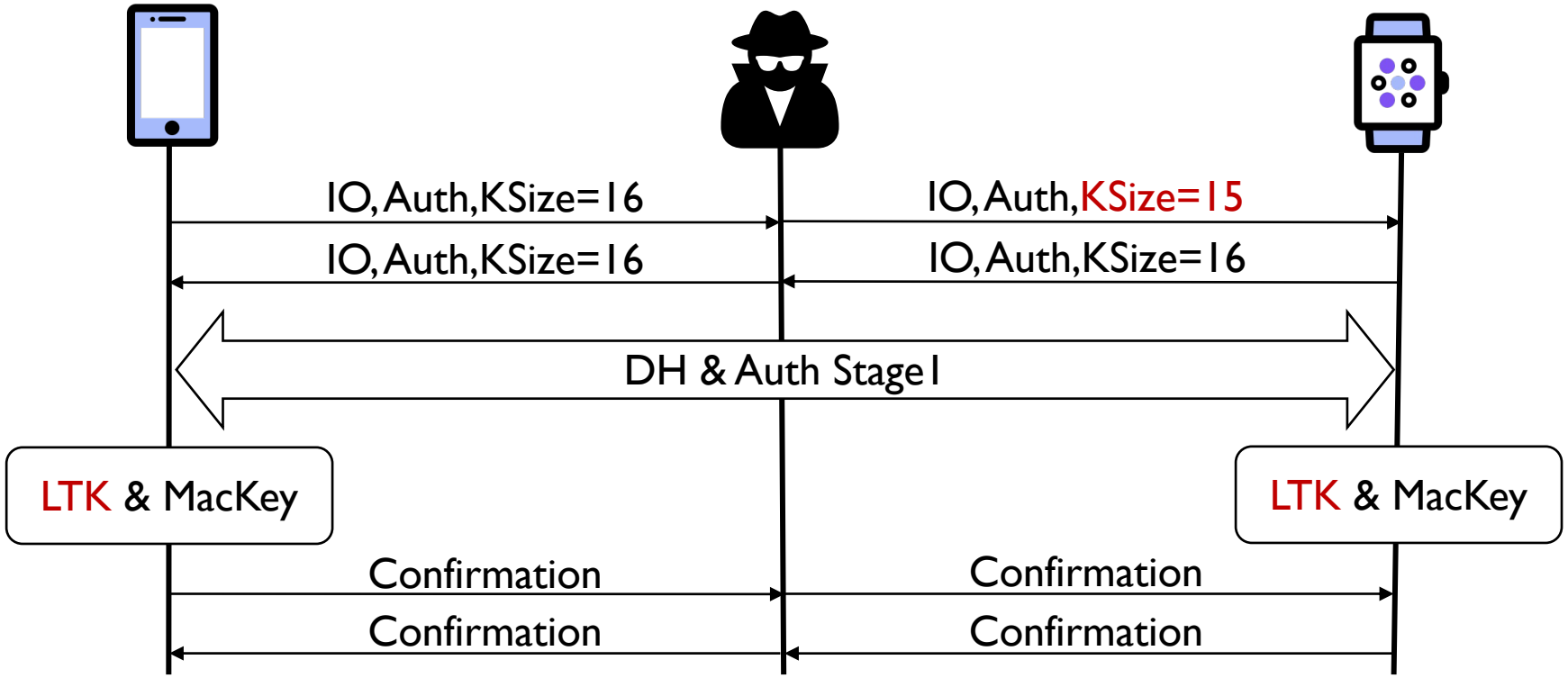


Countermeasures

- Higher Minimum Entropy
- Remove Entropy Negotiation

➢ Antonioli, D., Tippenhauer, N. O., & Rasmussen, K. (2020). Key negotiation downgrade attacks on bluetooth and bluetooth low energy. *ACM Transactions on Privacy and Security (TOPS)*, *23*(3), 1-28.

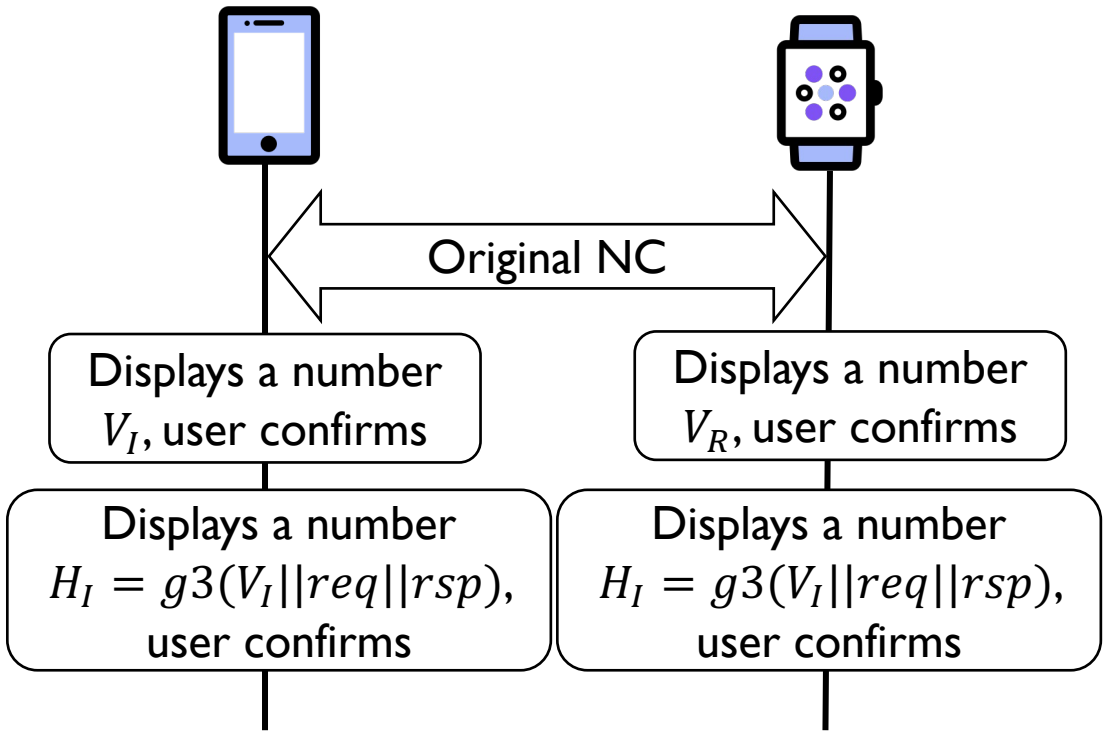
KeySize Confusion Attack



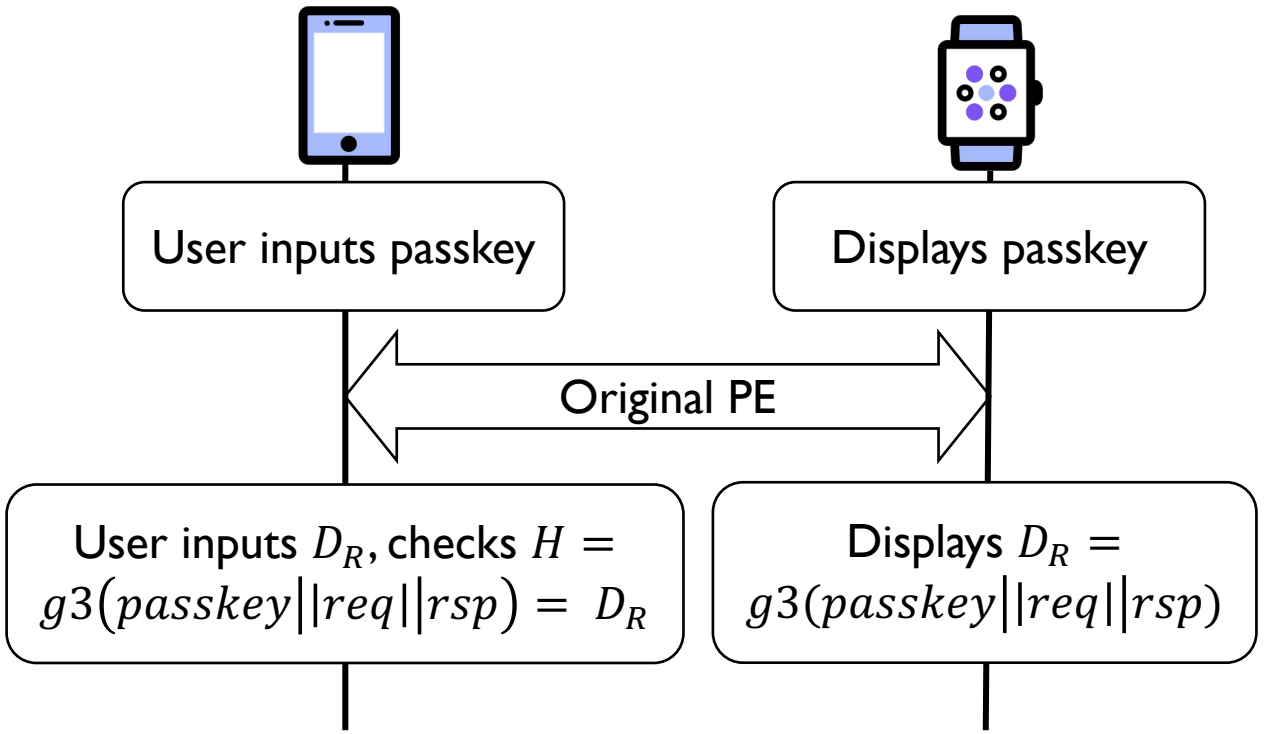
Interaction with the SIG

"We **agree** that the described scenario is a plausible means for a MITM to affect the establishment of a pairing or bonding between LE devices supporting and using LE Secure Connections pairing when the stored LTKs are generated and confirmed but nevertheless do not match because of different masked lengths."

Patching



Patched NC



Patched PE

The countermeasures had been verified under symbolic model.

Bluetooth SIG's Response

"As the described notification method occurs via information available at the host layer or above, implementations would be free to instigate this or similar notification method for users."

Thank you!

Contact: Min Shi, itachi@whu.edu.cn