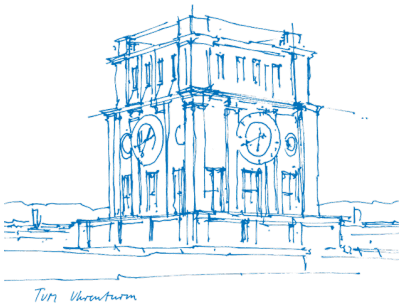
Chair of IT Security | Chair of Cyber Trust
School of Computation, Information and Technology
Technical University of Munich

Rediscovering Method Confusion in Proposed Security Fixes for Bluetooth

Maximilian von Tschirschnitz,
Ludwig Peuckert, Moritz Buhl, Jens Grossklags

School of Computation, Information and Technology
Technical University of Munich

February 25, 2025



3.8 Billion WiFi [6], 1 Billion Zigbee [2],
and 5.4 Billion Bluetooth [1] devices in 2023.
How to connect them?

3.8 Billion WiFi [6], 1 Billion Zigbee [2],
and 5.4 Billion Bluetooth [1] devices in 2023.
How to connect them securely?

That's why we developed Ad hoc Pairing Protocols

- Independent from external infrastructure.
- No pre-shared secrets.
- Devices interface directly (aided by user) to establish trust.

But: No single protocol works for all device combinations!
$\Rightarrow$ A *Connectivity Framework* like Bluetooth has to offer many Pairing Protocols

Investigating Bluetooth: A Classic Connectivity Framework

An Important Problem Emerged

Pairing Method Confusion	18/05/2020	SIG Security Notice	Core Spec, v2.1 to v5.2	CVE-2020-10134

2021 IEEE Symposium on Security and Privacy (SP)

Method Confusion Attack on Bluetooth Pairing

Year: 2021, Pages: 1332-1347
DOI Bookmark: 10.1109/SP40001.2021.00013

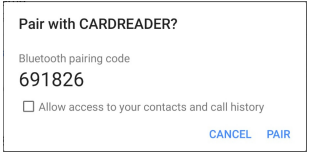
More Similar Problems Emerged

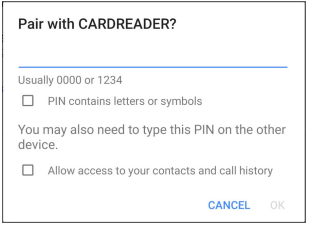
Pairing Method Confusion	18/05/2020	SIG Security Notice	Core Spec, v2.1 to v5.2	CVE-2020-10134
Pairing Mode Confusion in BLE Passkey Entry	09/12/2022	SIG Security Notice	Core Spec v4.0 to 5.3	CVE-2022-25836
Pairing Mode Confusion in BR/EDR	09/12/2022	SIG Security Notice	Core Spec v1.0B to 5.3	CVE-2022-25837

Short refresher on Method Confusion.

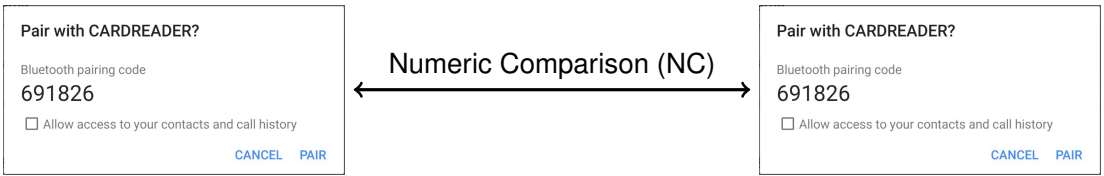
Bluetooth: Passkey Entry

Passkey Entry (PE)

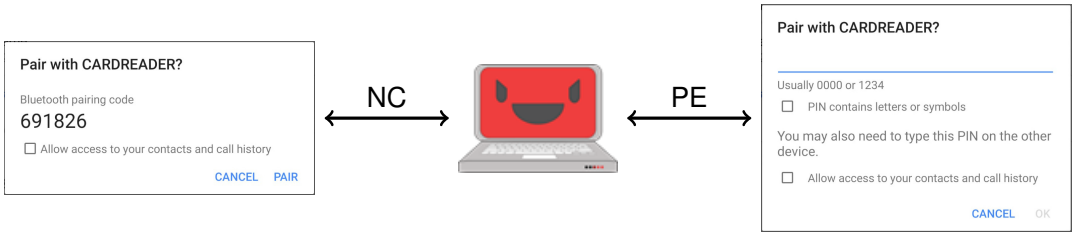




Bluetooth: Numeric Comparison



Original Method Confusion from S&P 2021 [4]



Ad hoc scenario permits protocol mismatch $\Rightarrow$ MitM

Is there a larger underlying issue?

Previous security proofs do not consider mismatching protocols!

We need a systematic approach: Modeling!

- We need a model that captures the reality of Method Confusion.
  - We focus on Bluetooth.
  - But our approach has broader applicability.
  - We encourage to inspect other protocol suites!

Basic Model of Ad Hoc Pairing

Ad Hoc Ecosystem

Basic Model of Ad Hoc Pairing

Ad Hoc Ecosystem

Third Party

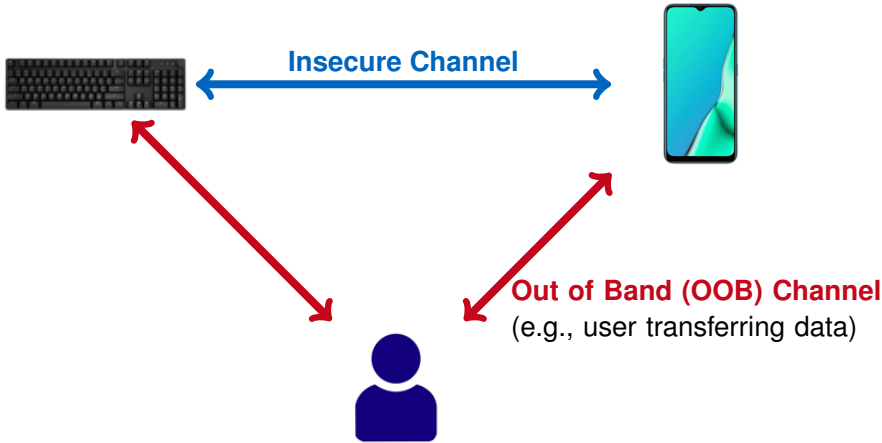
Basic Model of Ad Hoc Pairing

Ad Hoc Ecosystem

Third Party

Legitimate Pairing Partners (LPP)

Basic Model of Ad Hoc Pairing



Modeling Pairing Protocols

- Each Pairing Protocol has two *Roles*.
- When a device performs its side of the protocol this is a *Role Execution* (RE).
- A *Legitimate Pairing Partner* (LPP) can only run one RE at once.

Modeling the Adversary

- An Adversary may launch an RE on either LPP at will.
- After an RE has concluded they might launch another one.
- Multiple REs can be mixed and chained.

Modeling the Adversary

- An Adversary may launch an RE on either LPP at will.
- After an RE has concluded they might launch another one.
- Multiple REs can be mixed and chained.

$\Rightarrow$ To prove security any stacking of REs on both LPPs must be investigated.

Modeling the Adversary

- An Adversary may launch an RE on either LPP at will.
- After an RE has concluded they might launch another one.
- Multiple REs can be mixed and chained.

$\Rightarrow$ To prove security any stacking of REs on both LPPs must be investigated.

$\Rightarrow$ This (at first) seems like a lot of work.

Let's simplify!

- There are existing security proofs for most Pairing Protocols.
- Question: How could their assumptions be violated by mixing REs.
- Answer: Mixing REs only changes how data is handled by LPPs.
- Observation: Security proofs of Ad Hoc protocols never assume anything about data from the insecure channel.

Let's simplify!

- There are existing security proofs for most Pairing Protocols.
- Question: How could their assumptions be violated by mixing REs.
- Answer: Mixing REs only changes how data is handled by LPPs.
- Observation: Security proofs of Ad Hoc protocols never assume anything about data from the insecure channel.

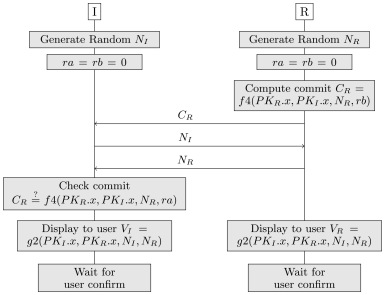
$\Rightarrow$ Security proofs do make assumptions about data coming from or going into the OOB channel. E.g. "the received data is a nonce", "the data I sent will be kept secret".

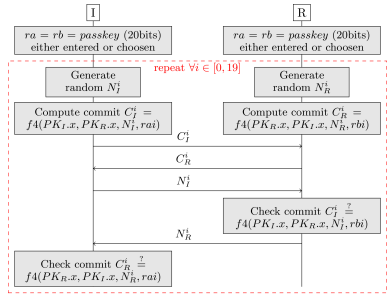
Let's simplify!

- There are existing security proofs for most Pairing Protocols.
- Question: How could their assumptions be violated by mixing REs.
- Answer: Mixing REs only changes how data is handled by LPPs.
- Observation: Security proofs of Ad Hoc protocols never assume anything about data from the insecure channel.

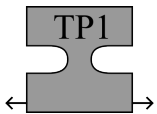
⇒ Security proofs do make assumptions about data coming from or going into the OOB channel. E.g. "the received data is a nonce", "the data I sent will be kept secret".
⇒ **We only need to care about mixing OOB interactions.**

Modeling the Role Executions
And their OOB Interactions

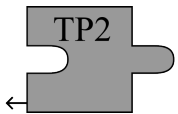




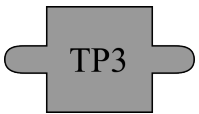
Modeling the Third Party/OOB
The User According to Bluetooth Specification



Receive value from both sides, and confirm if equal.

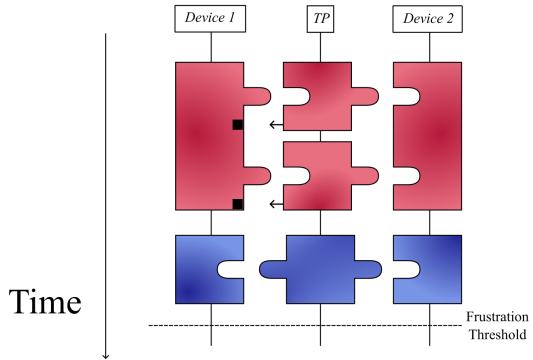


Receive value from one side, confirm, and forward to other side.

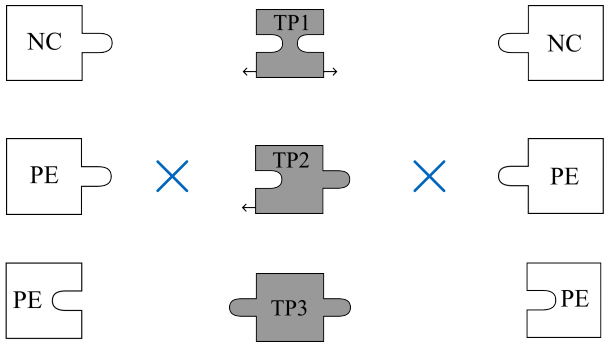


Enter random value on both sides.

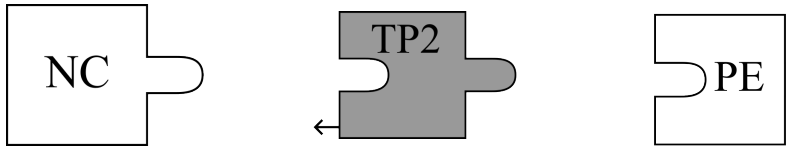
Attacker ‘Puzzles’ Against Us



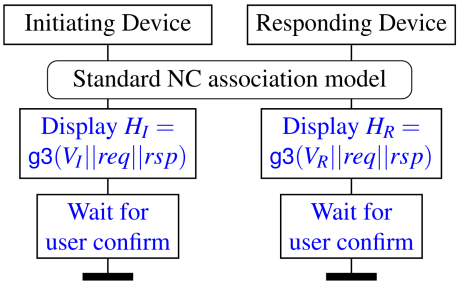
Let’s test all RE combinations in current Bluetooth



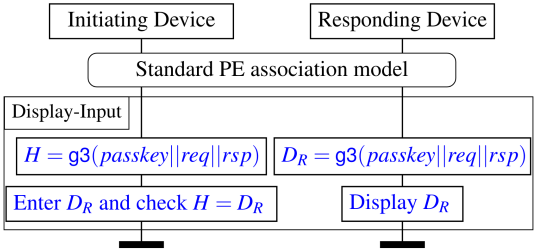
Verify MC from S&P 2021 [4]



Solution Proposal by Shi et al. [3]

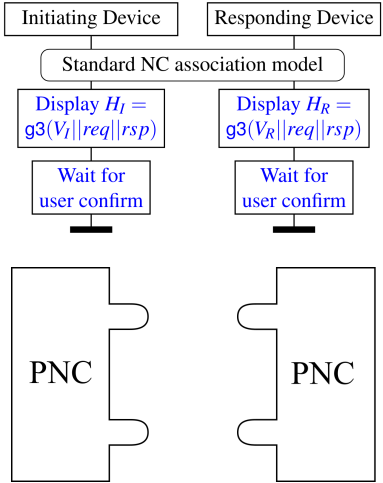


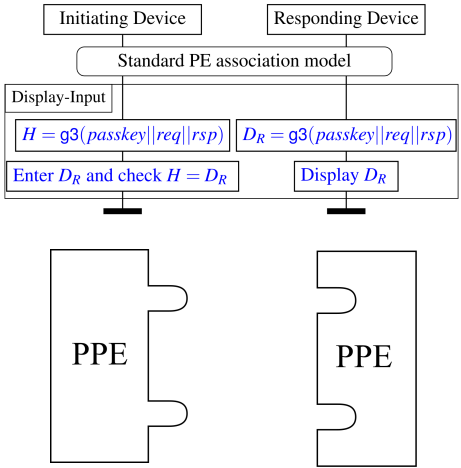
Patched NC (PNC)[3]



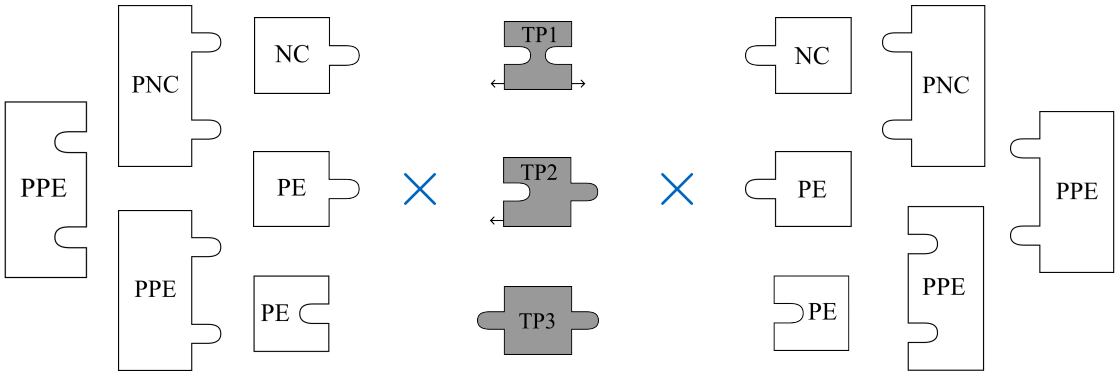
Patched PE (PPE)[3]

Investigating Shi et al. Proposal (Patched Pairing)



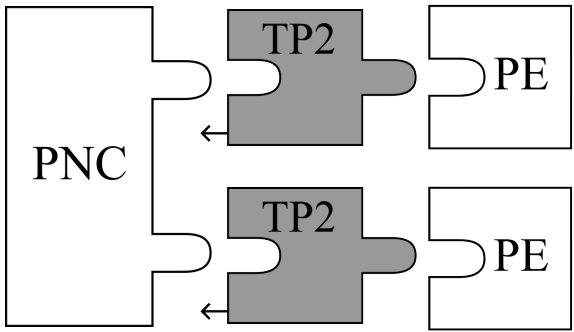


Let’s test all RE combinations in BT + Patched Pairing



Patched Pairing + Bluetooth

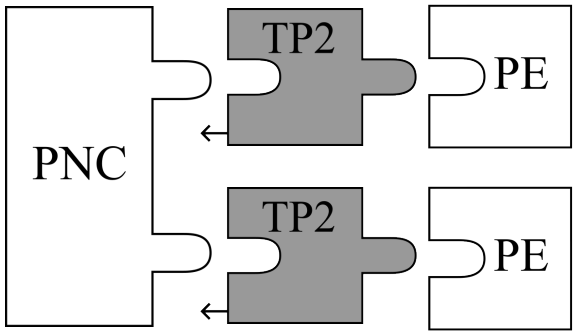
Still Vulnerable



MitM possible!

Patched Pairing + Bluetooth

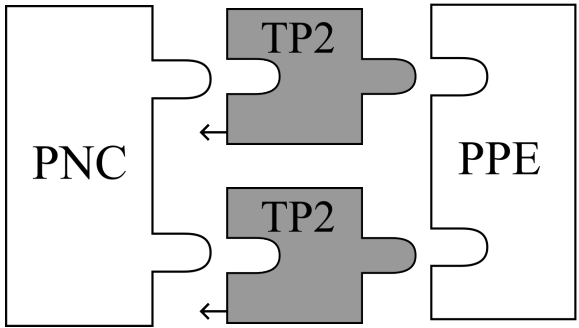
Still Vulnerable



We cannot fix Bluetooth by adding to it!

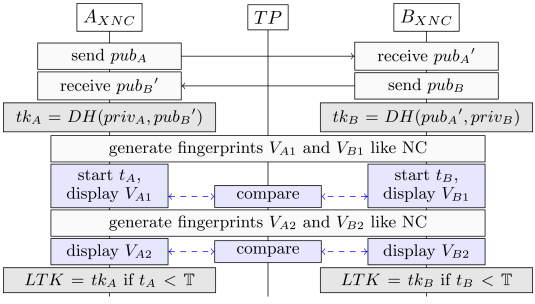
Patched Pairing as Alternative to Bluetooth (new Framework) ?

Patched Pairing as New Framework

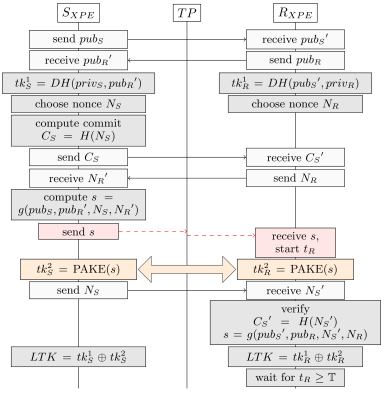


Even as standalone Framework, Patched Pairing is still insecure!

Our Solution
Xtended Pairing

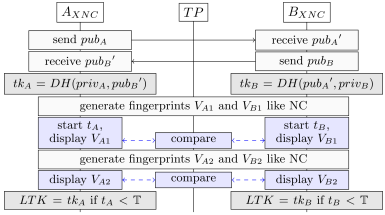


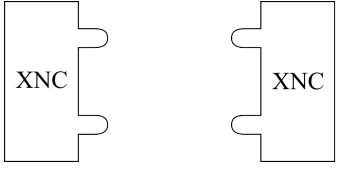
Extended NC (XNC)

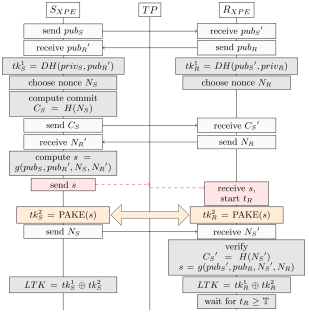


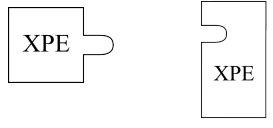
Extended PE (XPE)

Xtended Pairing









Formally proven secure in our broader threat model!

Conclusion

- We built a threat model to account for MC.
- We discover new MCs in recent solution proposals.
- We argue that we need a new framework.
- We propose XNC and XPE (support the same user and device landscape as Bluetooth).
- We formally prove the security of Xtended Pairing.
- We implemented and benchmarked all mentioned protocols [5].

Sources I

[1] Bluetooth SIG. *Bluetooth Market Update 2023*. https://www.bluetooth.com/2023-market-update/. 2023.

[2] Connectivity Standards Alliance. *Analysts Confirm Half a Billion Zigbee Chipsets Sold, Igniting IoT Innovation Figures to Reach 3.8 Billion by 2023*. https://csa-iot.org/newsroom/analysts-confirm-half-a-billion-zigbee-chipsets-sold-igniting-iot-innovation-figures-to-reach-3-8-billion-by-2023/. 2018.

[3] Min Shi et al. "Formal Analysis and Patching of BLE-SC Pairing". In: *32nd USENIX Security Symposium (USENIX Security)*. USENIX Association, 2023, pp. 37–52. ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/shi-min.

Sources II

[4] Maximilian Tschirschnitz et al. “Method Confusion Attack on Bluetooth Pairing”. In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1332–1347. URL: https://doi.org/10.1109/SP40001.2021.00013.

[5] Maximilian von Tschirschnitz and Moritz Buhl. *Advanced Method Confusion and X-Mitigations*. URL: https://github.com/maxdos64/advanced_mc.

[6] Wi-Fi Alliance. *Wi-Fi by the numbers: Technology momentum in 2023*. https://www.wi-fi.org/beacon/the-beacon/wi-fi-by-the-numbers-technology-momentum-in-2023. 2023.