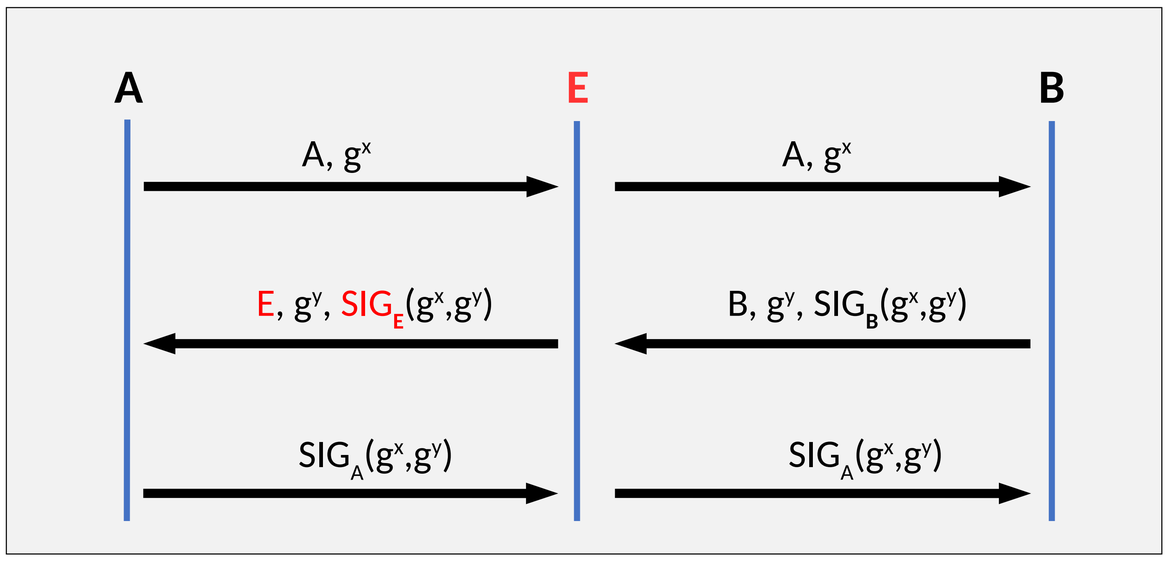
Misbinding Attacks on Secure Device Pairing and Bootstrapping

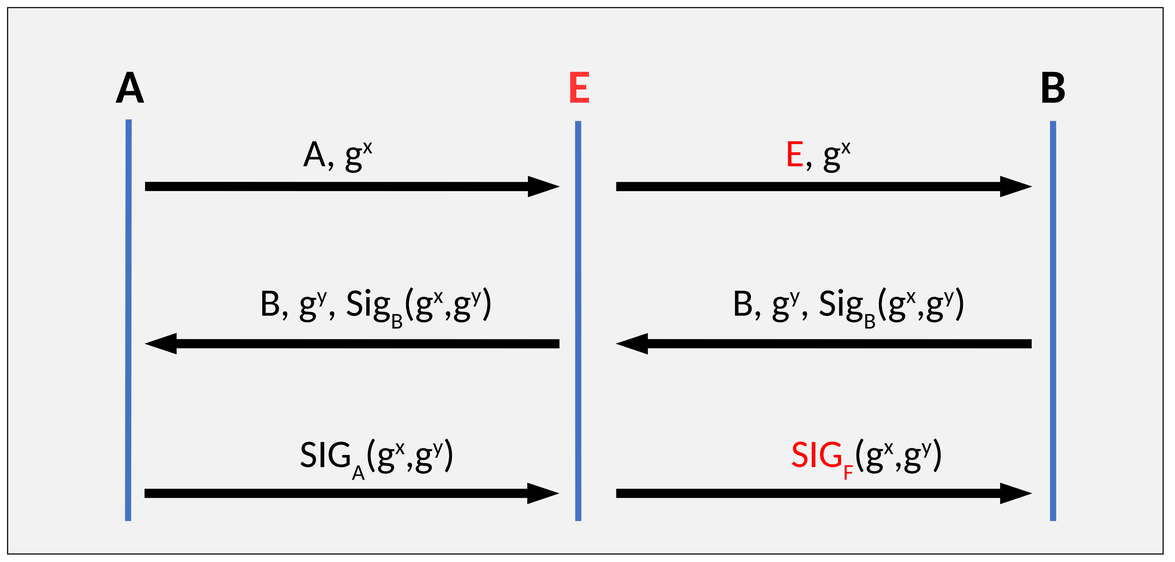
Aleksi Peltonen, Mohit Sethi and Tuomas Aura

Misbinding attack: **A** thinks that it is communicating with **E**, but is actually communicating with **B**

- Affects key exchange, secure device pairing and IoT bootstrapping protocols
- Requires **E** to be dishonest, **B** can be either honest or dishonest



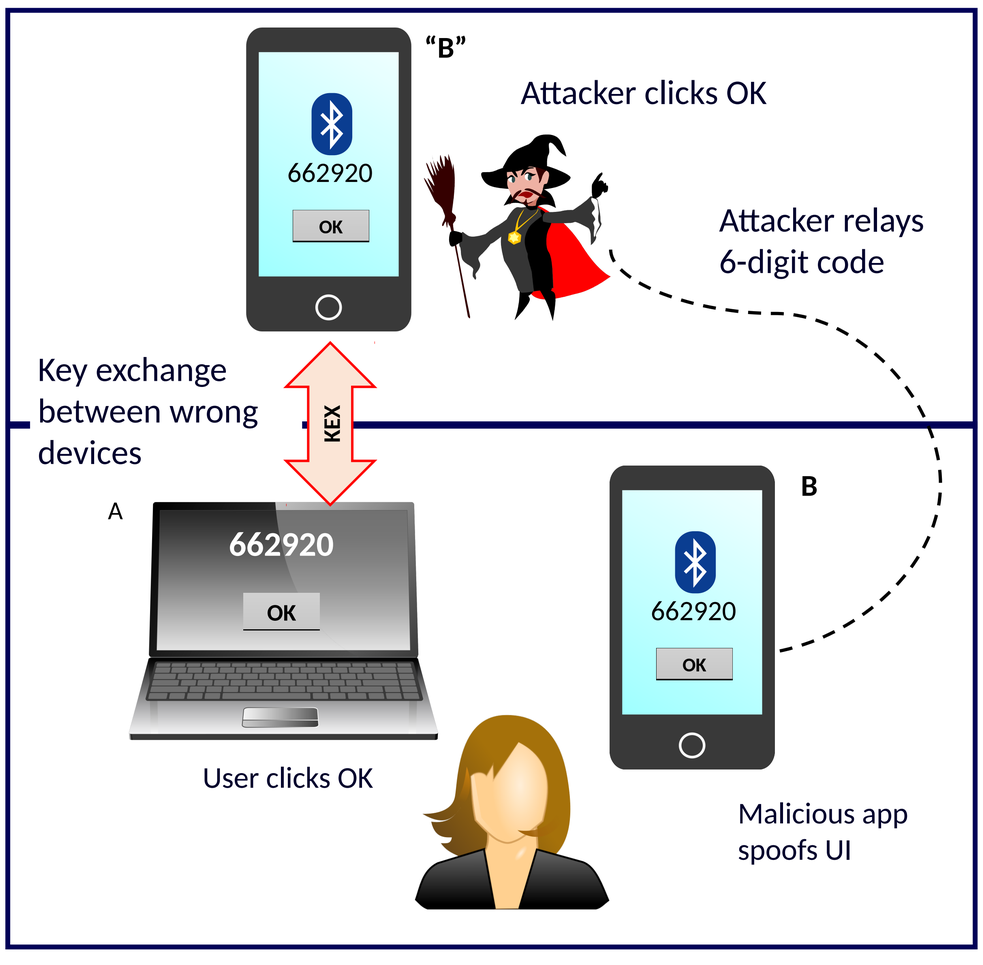
1) Misbinding of responder: **A** think that it's connected to **E**



2) Misbinding of initiator: **B** think that it's connected to **E**

- **Known since 1992** (STS, Diffie et al. 1992)
  - Different names over time: unknown key-share, misbinding, cuckoo..
- Motivated development of the SIGMA protocols (IKEv1, IKEv2)
- **Protocols without authenticated identifiers still vulnerable**
- **Formal modelling** of three protocols with ProVerif: Bluetooth, Wi-Fi Direct and EAP-NOOB
- Confirmed known attacks and discovered a new, **double misbinding** attack

CASE STUDY – Device Pairing with **Bluetooth**



Authentication by numeric comparison of 6-digit code.

Attack scenario:

User wants to pair devices **A** and **B**

1. Attacker makes compromised device **B** undiscoverable, user selects "**B**" instead.
2. The code derived by **A** and "**B**" is relayed and displayed on **E**.
3. User compares the codes and accepts.
4. User thinks that **A** and **B** are connected. In reality, **A** and "**B**" are connected.

Our model detected **five attack variants** for Blueooth.

Aalto University
School of Science and Technology

Contact: aleksi.peltonen@aalto.fi, mohit.sethi@aalto.fi, tuomas.aura@aalto.fi
Full report: https://arxiv.org/abs/1902.07550