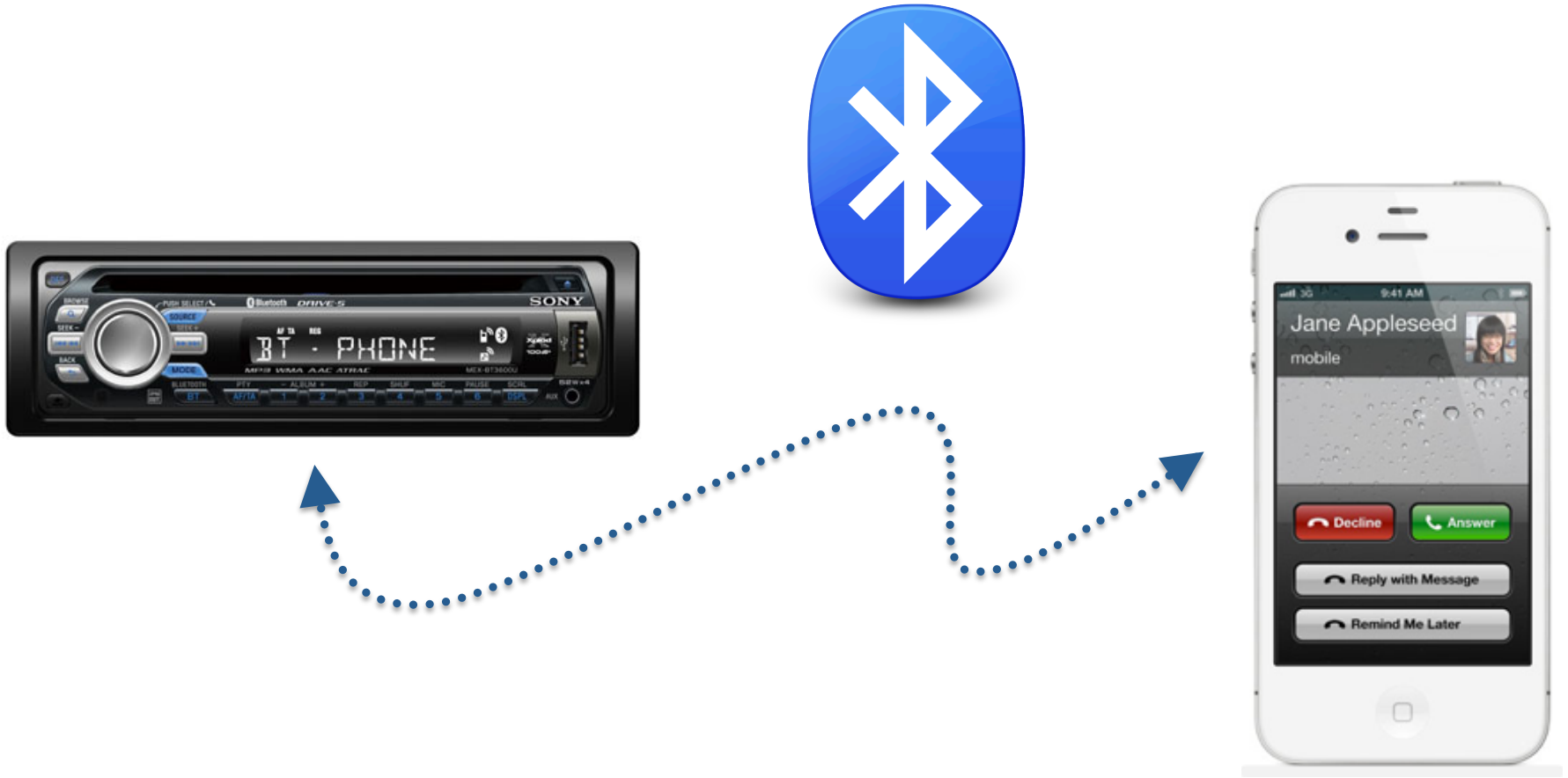
Secure Device Pairing

What is device pairing?

What is device pairing?



What is the problem?

- The wireless communication channel is relatively easy to **eavesdrop** upon and to **manipulate**.

What is the problem?

- The wireless communication channel is relatively easy to **eavesdrop** upon and to **manipulate**.
- Device pairing is susceptible to **Man-in-the-Middle** (MiTM) and **Evil Twin** attacks.

What is the problem?

- The wireless communication channel is relatively easy to **eavesdrop** upon and to **manipulate**.
- Device pairing is susceptible to **Man-in-the-Middle** (MiTM) and **Evil Twin** attacks.

In order to create a secure communication channel the devices must be securely initialized, in a such a way that the user is involved in the pairing process

Possible way to achieve secure pairing

- Smartphones pairing: *Shake Well Before Use*

Possible way to achieve secure pairing

- Smartphones pairing: *Shake Well Before Use*
- Vehicle-to-mobile pairing: a protocol which leverages cryptographic schemes based on various out-of-band channels

Contact info:

Elena Pagnin (elenap@chalmers.se)

Katerina Mitrokotsa (aikmtr@chalmers.se)