16:00

←

Olga Sanina

last seen at olga.sanina@tu-darmstadt.de

⚠ Privacy in user-based key exchange protocols in mobile devices

🔒 Bluetooth and Wi-Fi might be less secure than you think.

Learn more

How do you judge?

By conducting **cryptographic analysis**: (1) defined desired *security guarantees*; (2) specified *adversarial abilities*; (3) *[dis]proved* the protocol achieves the guarantees in this model.

BACK Was there nothing like that before?

Sure! But **previous analyses** considered *stand-alone protocols*, didn’t cover *new attacks or versions*, modelled the protocols *not close to the standards*.

13 June 2022

📊 What are the results?

Bluetooth is secure in *trust-on-first-use* (TOFU) model. Results on **Wi-Fi** are on the way, stay tuned! SOON

What is a TOFU-model?

TOFU-model distinguishes between *initial first connections* with passive (👂) adversaries and *reconnections* with active (🔁 🔀 ⏏ ⏹) adversaries.

Trust is clear, what about privacy?

Bluetooth **MAC-address randomisation** mechanism provides *decent outsider privacy* when ruling out physical characteristics.

☺ Bluetooth is secure 😊 … but in reconnections 😟

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users