Contextual Security Project
Secure Systems Group, Aalto University

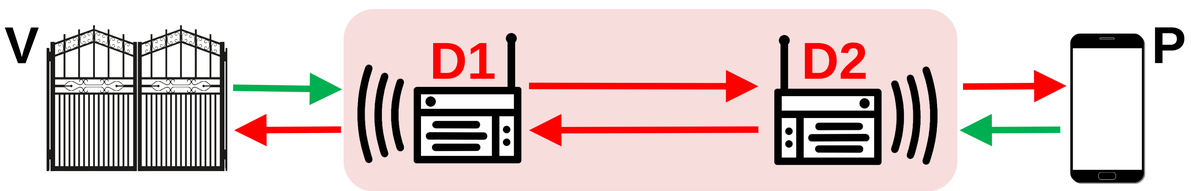
CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

Mika Juuti, Christian Vaas, Ivo Sluganovic, Hans Liljestrand, N. Asokan & Ivan Martinovic

STASH: Securing Transparent Authentication using prover-side proximity verification

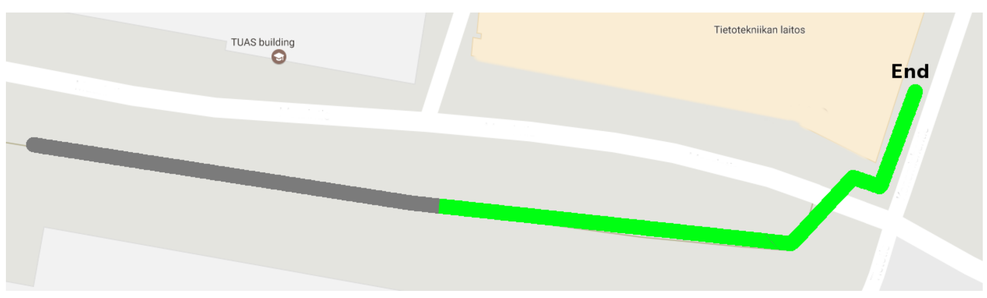
Relay Attacks against Transparent Authentication

- Users gain access to a verifier device **V** when it detects a user-equipped prover device **P** nearby
- Relies on wireless cryptographic authentication
- Examples: BlueProximity, Keyless Entry, etc.
- Inherently assumes spatial proximity of user can be sensed with external measurements on **V**
- Attacker can misuse proximity assumption to gain access to verifier, by using a pair of relay devices (D1 & D2)



Solution: trajectory recognition on prover

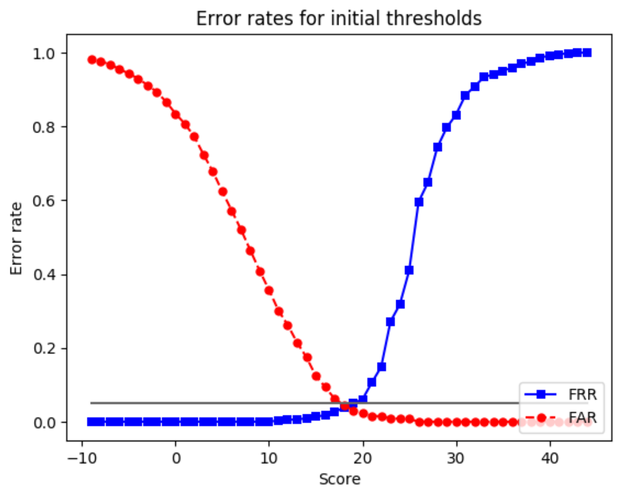
- Attack can be resisted if prover smartly moderates its participation in protocol
- We use internal sensors on prover to model *approach trajectory* for this decision



- Prover associates authorized reference trajectories with a verifier **V**
- Prover compares current trajectory to references
- High similarity:
  → transparent authentication *permitted*
- Low similarity:
  → fall-back to manual authentication

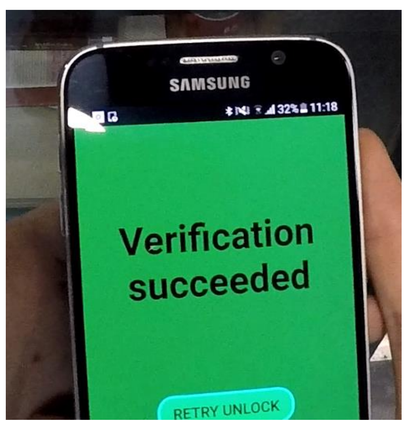
Security & Usability trade-off

- Trajectory represented as a sequence of turns and movements: e.g. MMMLLLLLMM
- String similarity metric: Needleman-Wunsch
- High thresholds:
  increase security (lower FAR), but decrease usability (higher FRR)
- Empirical optimal decision threshold



Android prototype

- Proximity sensing by NFC or Bluetooth
- Power consumption low
- Memory buffer requirements ~ 5MB/h



Performance

- Reference paths of length 2-6 minutes:
  FAR 4-7%, FRR 4-6% on *first* repetition
  FAR 2-5%, FRR 2-3% with five repetitions
- Works already from the first try
- Performance increases with more repetitions

Aalto University
UNIVERSITY OF OXFORD
ACADEMY OF FINLAND
EPSRC Engineering and Physical Sciences Research Council