Context-based Authentication and Device Pairing

BANDANA – Body Area Network Device-to-device Authentication using Natural gAit
[PerCom 2017]

Concept

- Connecting on-body devices: ad-hoc and secure
- Gait fingerprinting based on gait cycle variation
- Using error correcting code to derive secret keys

Evaluation

- Evaluating the similarity of gait fingerprints on public datasets: intra-body vs inter-body
- Proximate body parts achieve more similar fingerprints, e.g. arm – chest vs arm – shin

Security

- Gait fingerprints have high entropy: assessed by the DieHarder random number test suite
- Video-based attacks:
  - Using high-speed camera
  - Required extensive manual effort to estimate acceleration readings

Audio Pairing
[TMC 2013]

Image-based Passwords
[PerCom 2017]

Ambient Intelligence Group
http://ambientintelligenc.aalto.fi/
Stephan.Sigg@aalto.fi
Le.Ngu.Nguyen@aalto.fi