DEPARTMENT OF
COMPUTER
SCIENCE

Broken Hearted: How to Attack ECG Biometrics

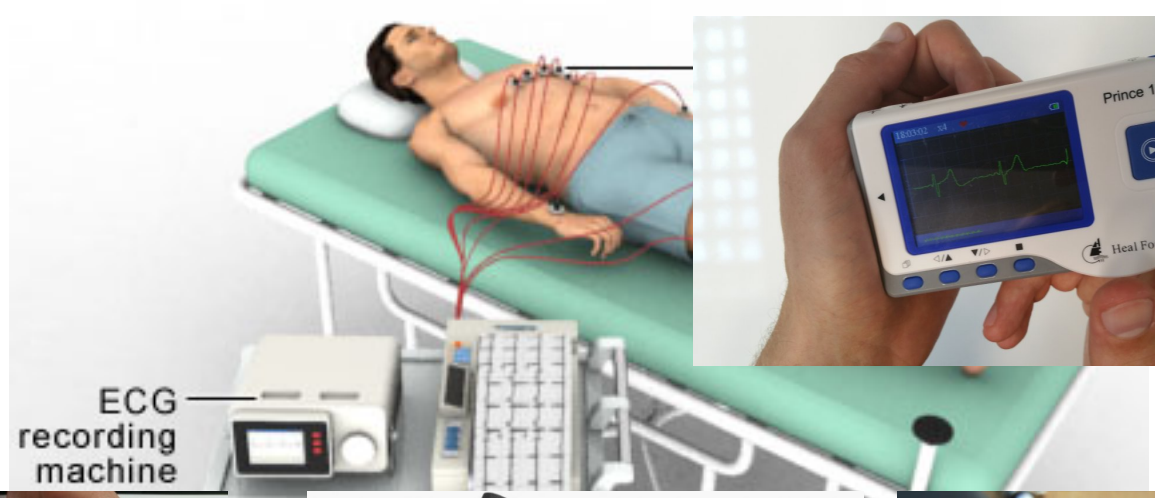
Simon Eberz[¶], **Nicola Paoletti**[¶], **Marc Roeschlin**[¶], **Andrea Patane**[§], **Marta Kwiatkowska**[¶], **Ivan Martinovic**[¶]

[¶]Department of Computer Science
University of Oxford, UK

[§]University of Catania, Italy

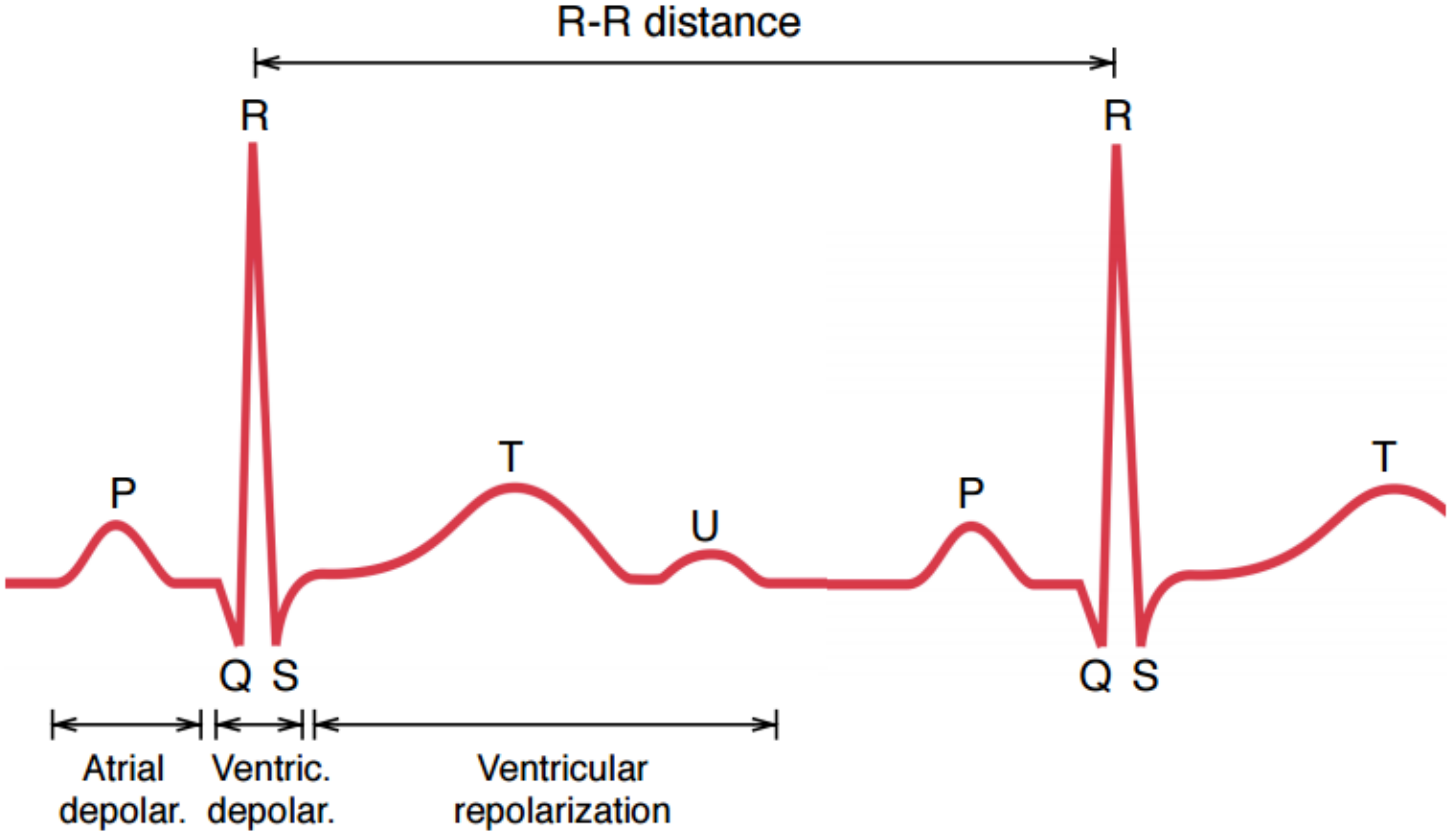
Background - ECG

- Recording of the heart's electrical activity
- Electric potential differences measured on a person's skin
- Most common use: Medical diagnosis



Background – ECG Biometrics

- Generic waveform common to healthy individuals
- Individual differences in amplitude, duration and distance
- Significant body of academic work



Background – Nymi Band

Background – Nymi Band (2)

- Communication with all Bluetooth/NFC devices (NEAs)
- Trialled for contactless payments and online banking

Threat Model

- To break the Nymi Band, the attacker needs to
  - Obtain access to the band itself
  - ~~Obtain access to the NCA (e.g., user's smartphone)~~

  - Circumvent ECG-based authentication

Focus of this work

A Presentation Attack Against ECG

- Goal: Impersonation of the legitimate user
- ECG is available through a number of sources

Printed ECG Signal

E-health

Fitness Devices

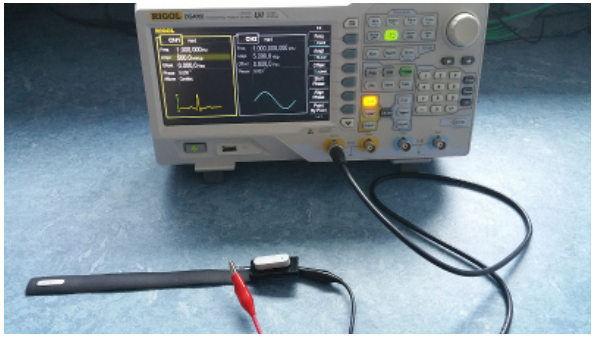
- Different measurement locations and device properties!
- Cross-Device attacks

Collecting Data for the Attack

- 41 Participants
- 3 different devices
- 5 measurement modes

Signal Injection Methods

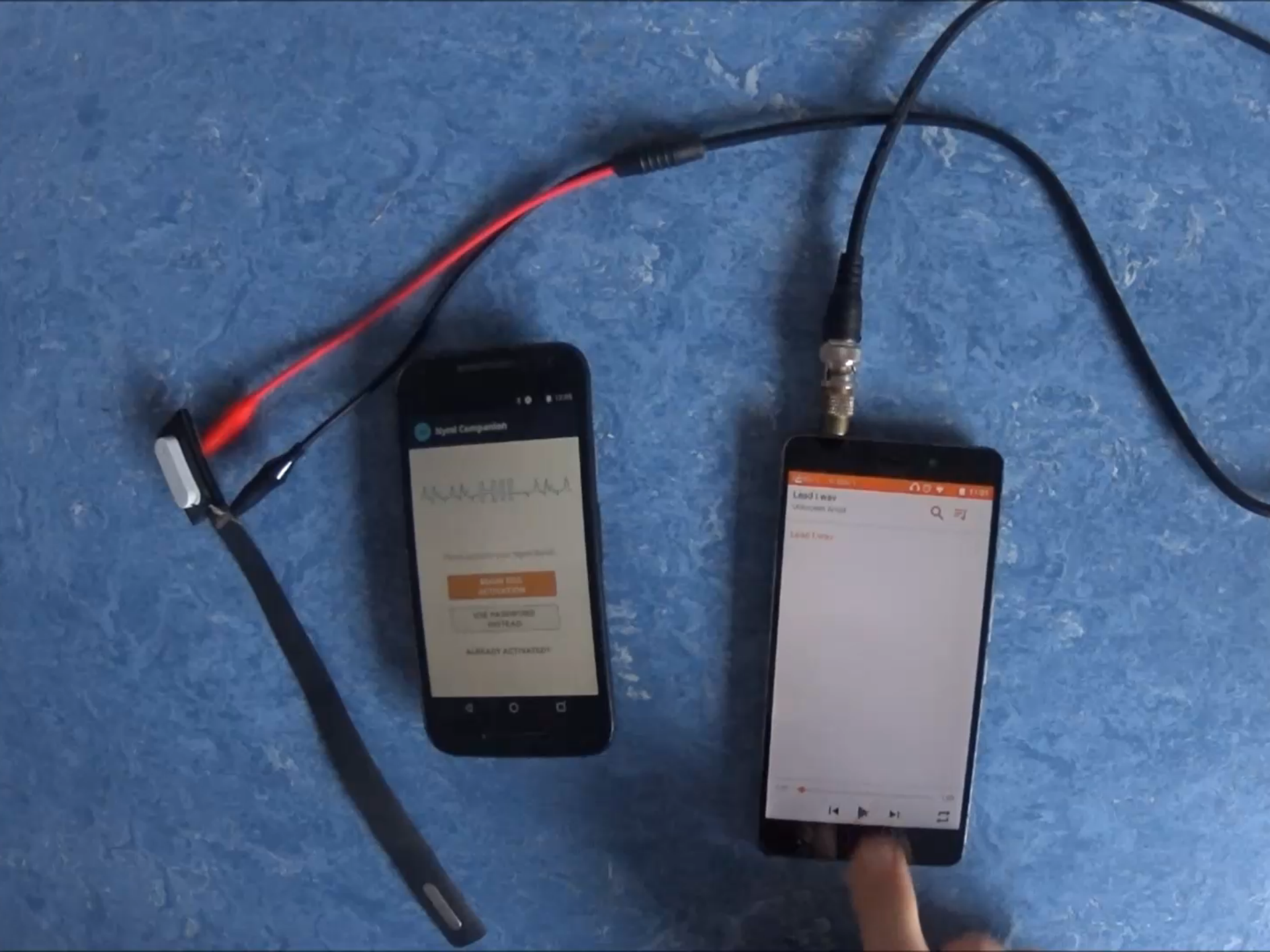
- Hardware arbitrary waveform generator



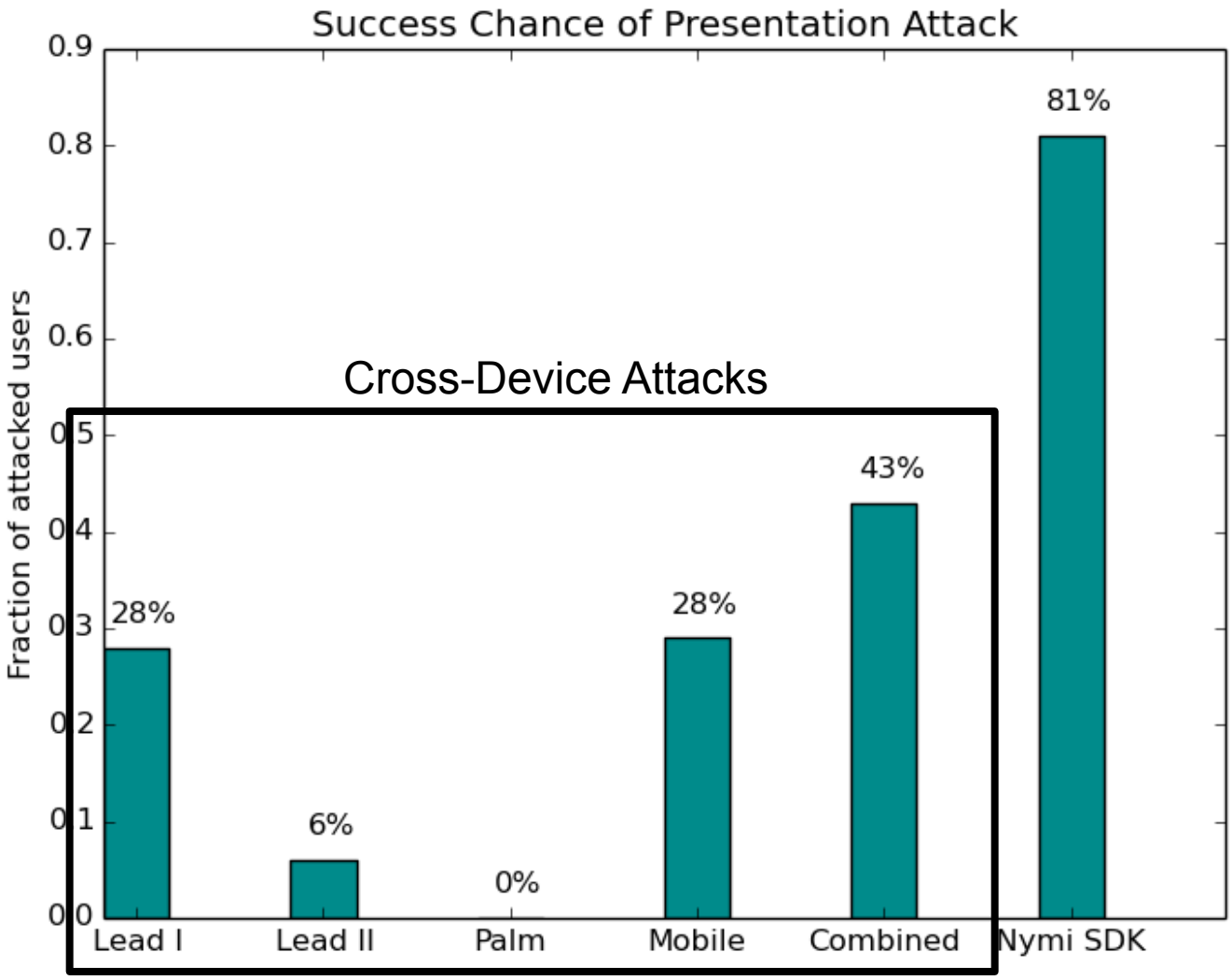
- Laptop soundcard with SW-based waveform generator

- Playback of .wav-encoded ECG signal

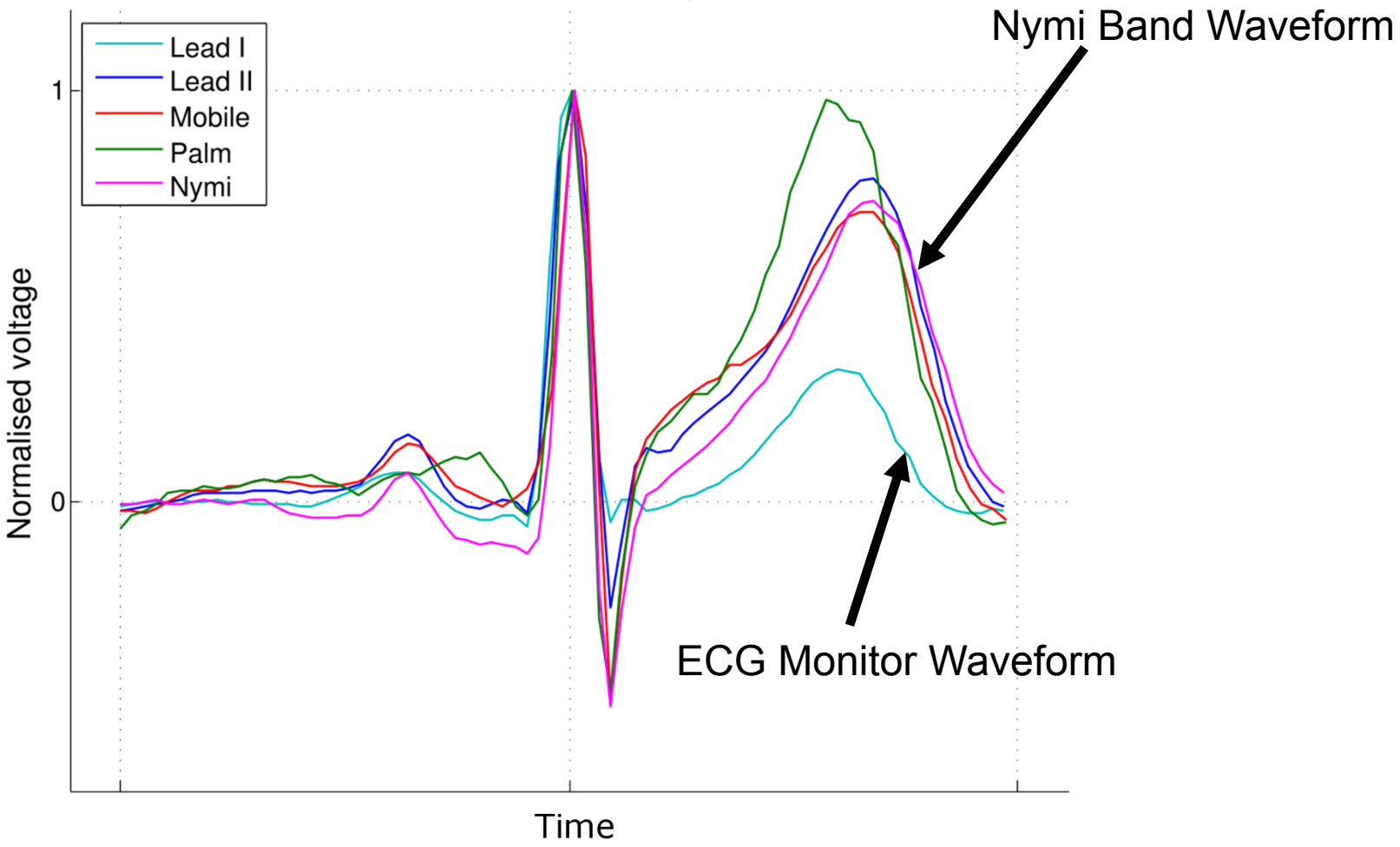
“There is currently no known means of falsifying an ECG waveform and presenting it to a biometric recognition system. ”


Xyrid Companion
Lead I.wav

Initial Results

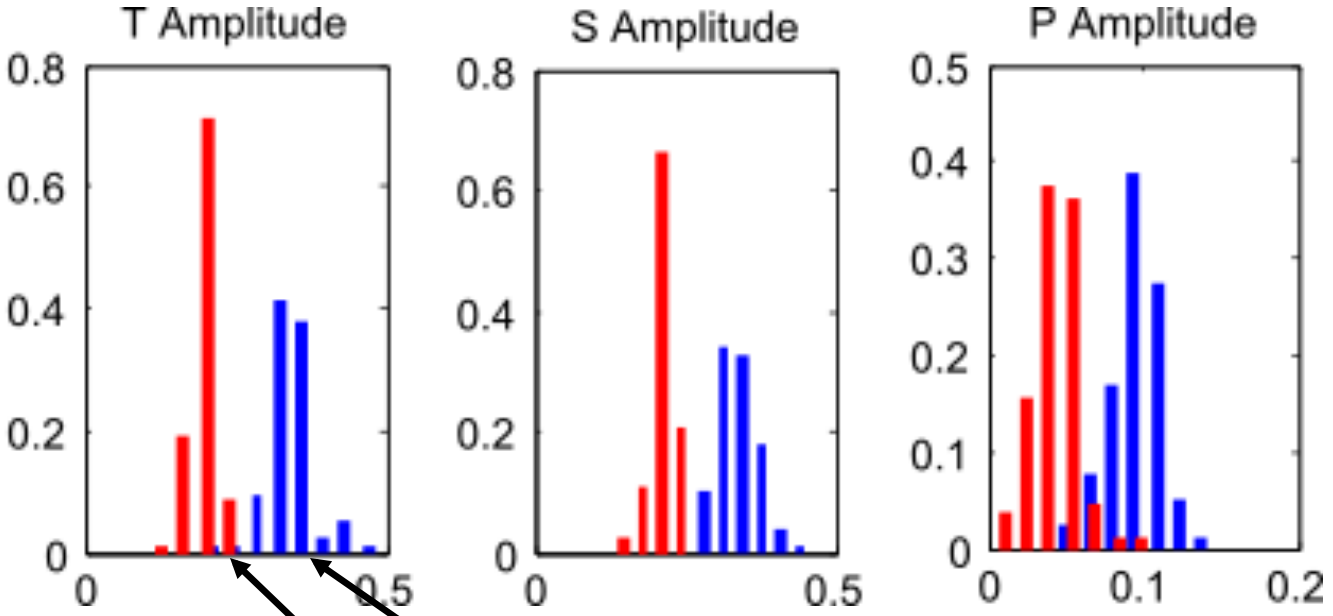


The Challenge of Cross-Device Attacks



- Different waveform morphology between devices!

Training a Cross-Device Mapping



SOURCE ECGs $\{\text{ECG}_i^S\}_{i\in I}$

TARGET ECGs $\{\text{ECG}_i^T\}_{i\in I}$

ECG DETECTION AND FEATURES EXTRACTION

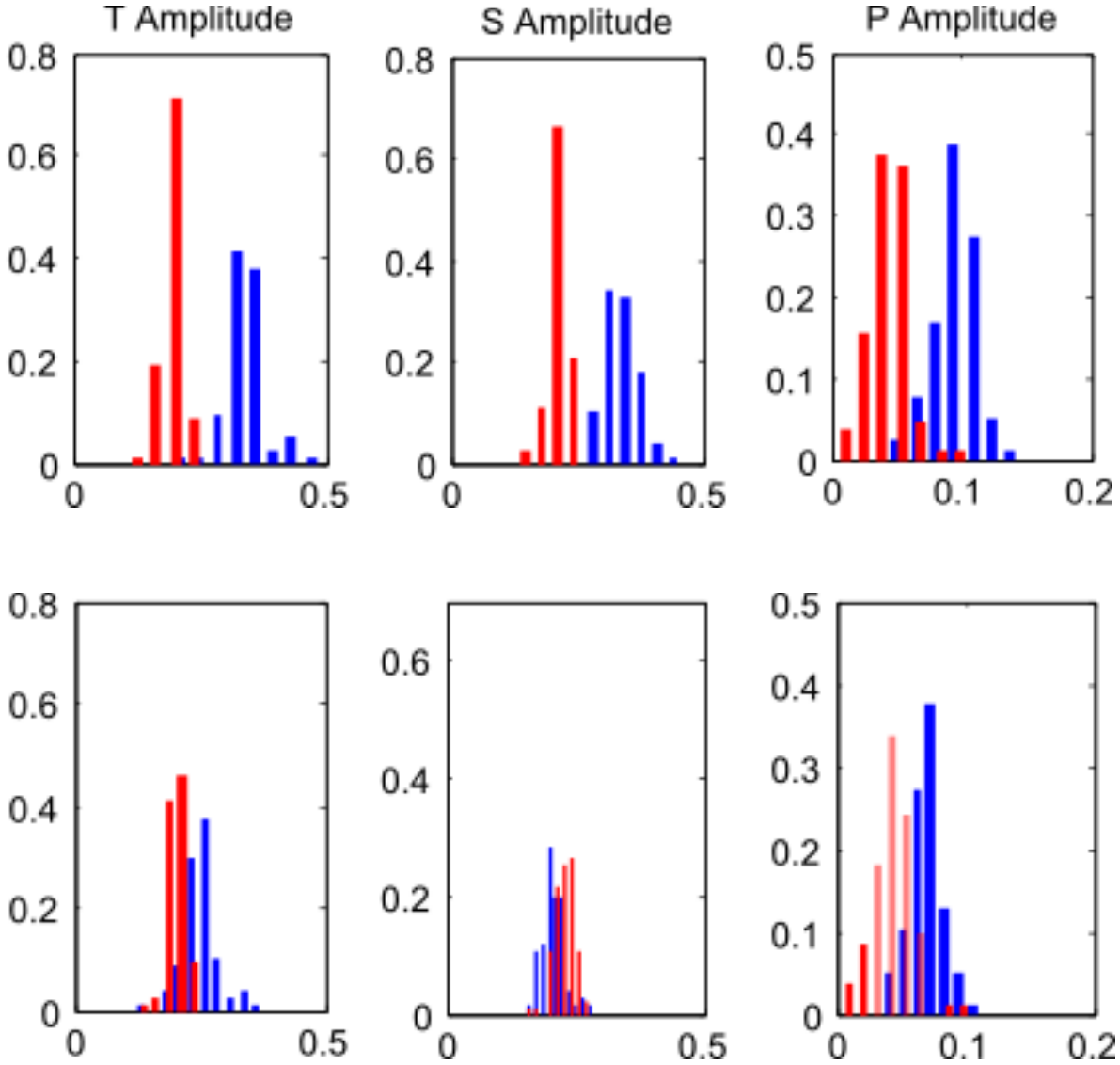
SOURCE FEATURES DISTRIBUTIONS $\{\mathcal{D}_i^S\}_{i\in I}$

TARGET FEATURES DISTRIBUTIONS $\{\mathcal{D}_i^T\}_{i\in I}$

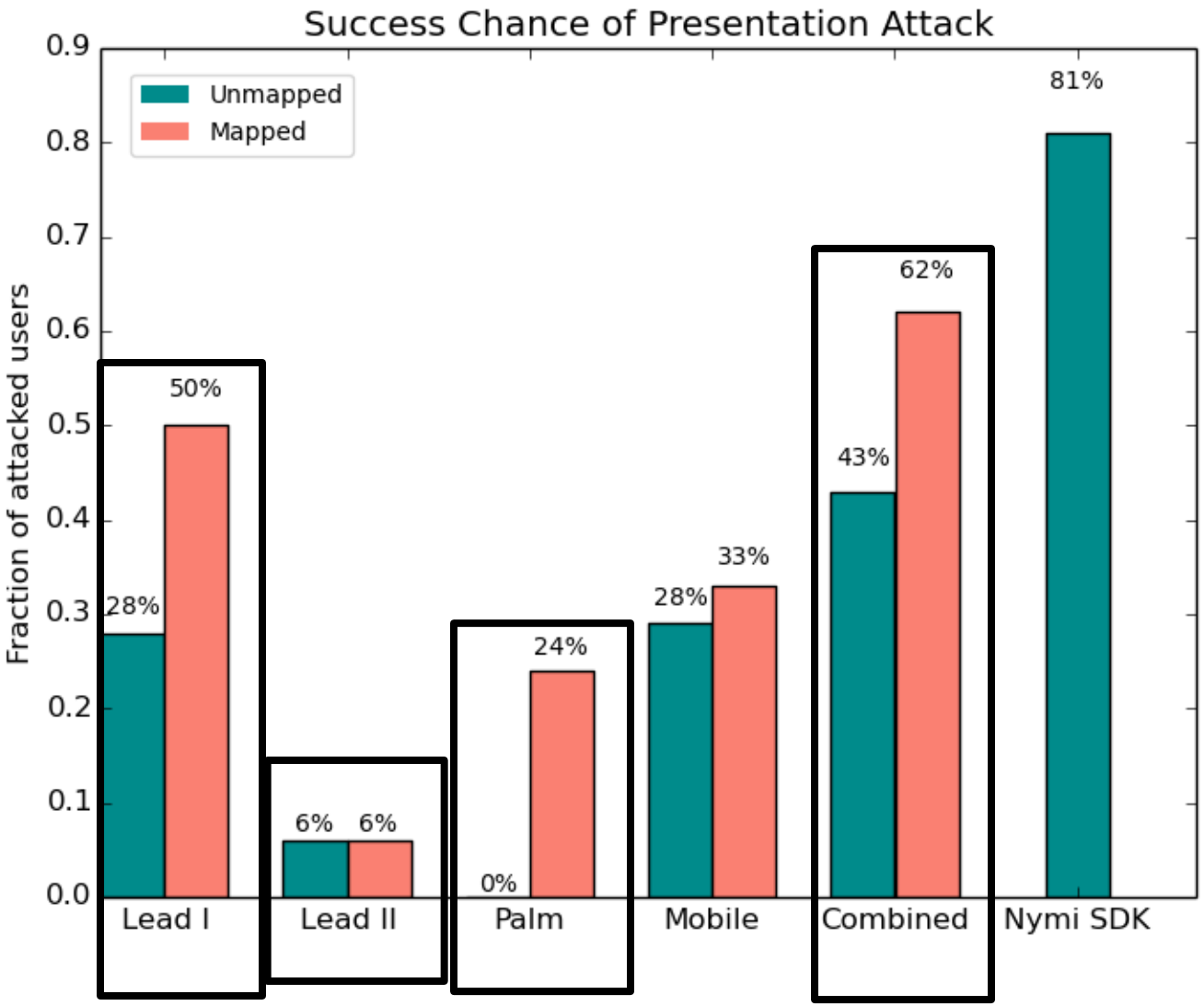
OPTIMISATION $\min \sum_i d\left(\mathbf{f}(\mathcal{D}_i^S), \mathcal{D}_i^T\right)$

MAPPING $\mathbf{f}$

Training a Cross-Device Mapping - Results



Final Results



Conclusion

- Successful presentation attack against ECG biometric
- Wide variety of data sources suitable for attacks
- Remarkably low technological barriers
- Future Work
  - Further improve cross-device mapping
  - Can very old data be used for the attack?

Conclusion – Questions?

- Successful presentation attack against ECG biometric
- Wide variety of data sources suitable for attacks
- Remarkably low technological barriers
- Future Work
  - Further improve cross-device mapping
  - Can very old data be used for the attack?

Thank you for your attention. Questions?

simon.eberz@cs.ox.ac.uk