Aalto University
School of Electrical
Engineering

Usable Security – Raise the bar with implicit device pairing

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

09.10.2017

MEMORY IS A LIMITED RESOURCE

WE USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS

SECURITY SHOULD NOT COMPROMISE EASE OF USE


WHAT IS USABLE SECURITY

Open your car from correlation in handle movement and acceleration on your watch


Securely synchronize items in your shopping list with those in your shopping basket

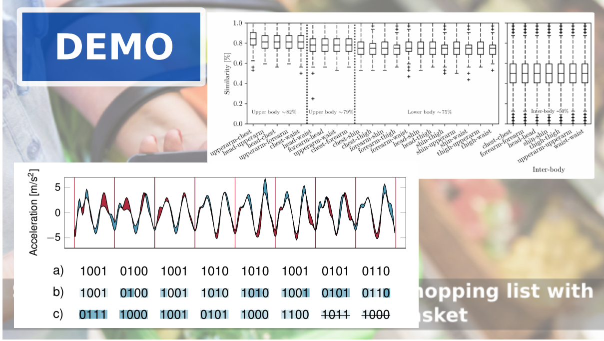
Exploit your heartrate to pair with devices attached to and inside your body.

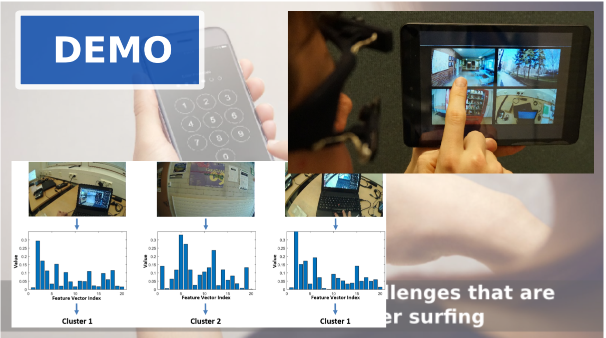

Securely share joint resources
conditioned on proximity

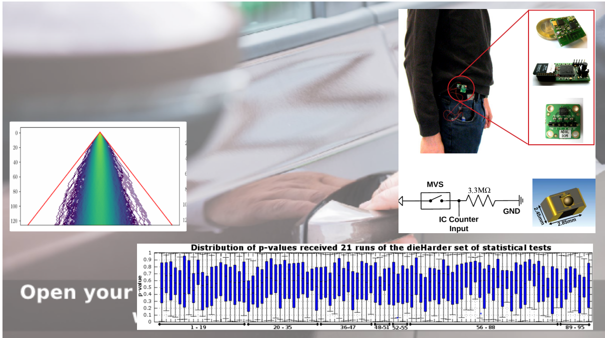
Implicit, always fresh login challenges that are resistant against shoulder surfing

http://ambientintelligence.aalto.fi


DEMO
Similarity of fingerprints from Nexus S and Nexus One devices
Median fraction of identical bits in fingerprints
Distance between devices [cm]
Before alignment
After alignment with extracted pattern
After alignment with arbitrary pattern
AdhocPairing
Connected Devices
No device connected
Nexus S
94:63:D1:5D:4D:70
Status Board
APActivity: TimeOffset is set to 5640
15:41:30.778
Nexus S: Time offset = 2517
15:41:48.077
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
15:41:57.961
AudioFingerprint.RecordThread: recorded 289958 shorts out of desired 289958 shorts
re joint resources
ed on proximity


DEMO
Similarity [%]
Upper body ~82%
Upper body ~79%
Lower body ~75%
Inter-body ~50%
Inter-body
Acceleration [m/s²]
a) 1001 0100 1001 1010 1010 1001 0101 0110
b) 1001 0100 1001 1010 1010 1001 0101 0110
c) 0111 1000 1001 0101 1000 1100 1011 1000
hopping list with
sket


DEMO
Value
Feature Vector Index
Cluster 1
Cluster 2
Cluster 1
llenges that are
r surfing


MVS
3.3MΩ
GND
IC Counter Input
2.85mm
Distribution of p-values received 21 runs of the dieHarder set of statistical tests
p-value
1 - 19
20 - 35
36-47
48-51
52-55
56 - 88
89 - 95
Open your

Thank you!

stephan.sigg@aalto.fi

http://ambientintelligence.aalto.fi