

# Evaluation of the security of smartwatch communication

Security of Systems & Networks

James Gratchoff, Harm Dermois, Florian Ecard



System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

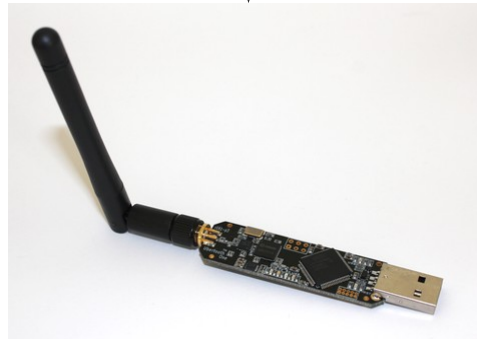
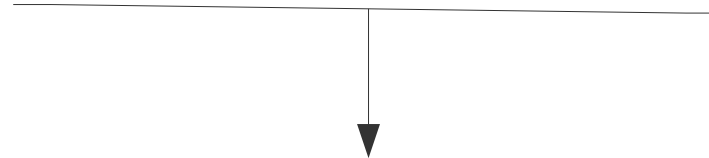
# Evaluation of the security of smartwatch communication

## Research question

- How secure is the communication ?
- Is it possible to eavesdrop any data?
- Is it possible to change the content of the data?
- How the vulnerabilities found (if any) could be addressed?



# Devices used during the investigation



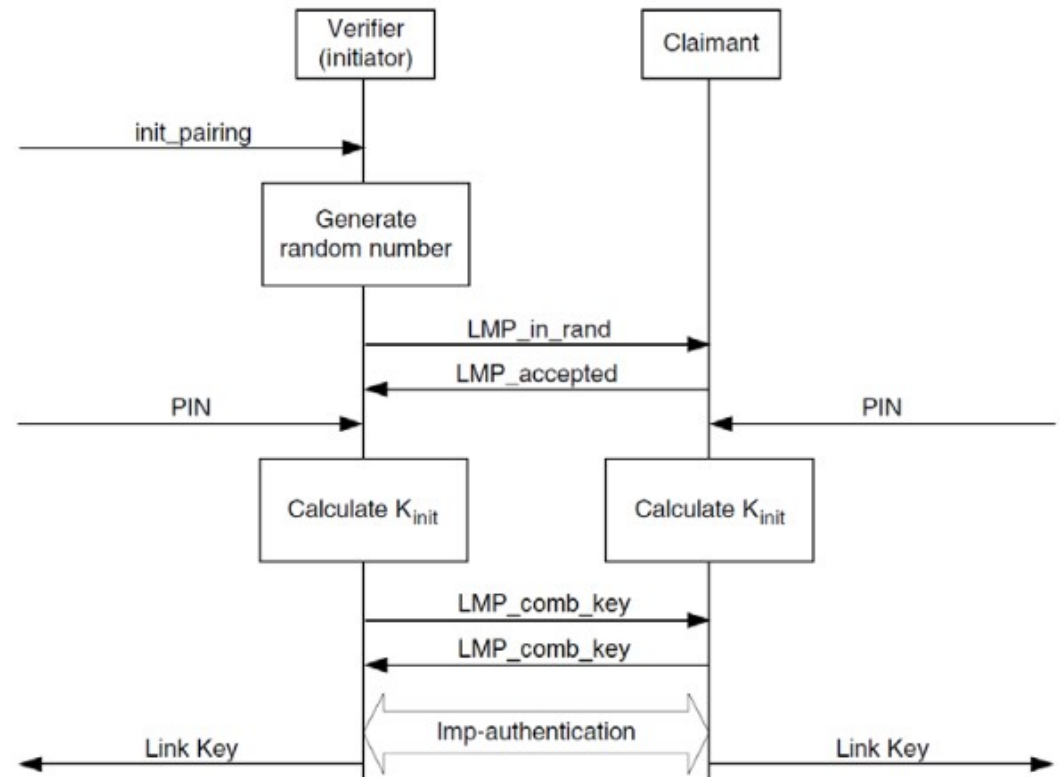
System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

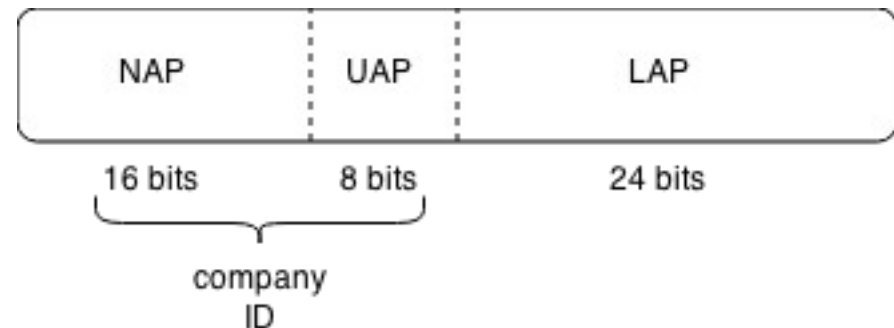
# Bluetooth security and pairing process

## LMP & its limitations



# Ubertooth

Kickstarter  
Passive/promiscuous  
Following devices  
Decrypting packets



System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

# Smartwatch and apps

Bluetooth 3.0  
Smart connect  
Pre-installed apps  
SDK



System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

# Android device

Android 4.2/4.4

BT snoop

Most apps do not work



System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

# Traffic analysis from the Ubertooth

Only discovery  
Poll and Null  
Link control



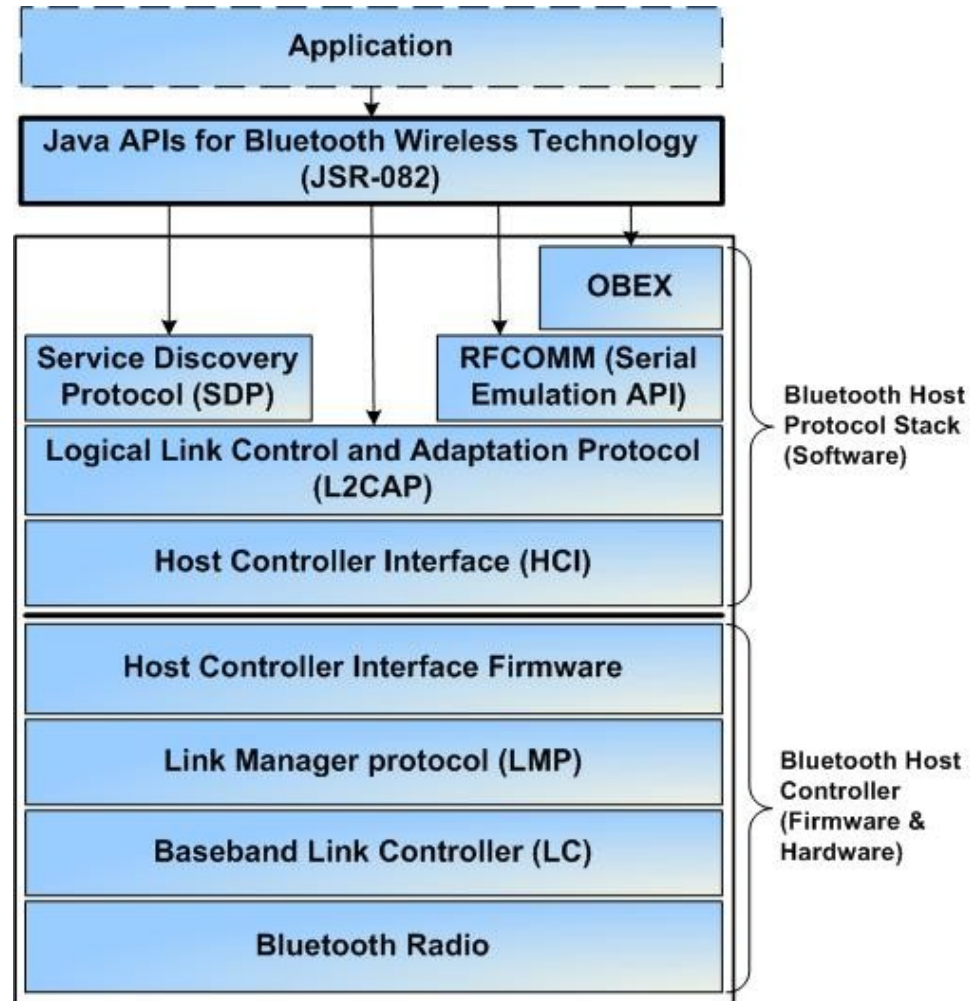
System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM



# Bluetooth stack



# Traffic analysis from the HCI

- All the traffic is in clear text
- Many parameters can be output from here
- No correlation possible from what we saw at the RF level



# Pairing process analysis

- Input/Output capabilities
  - LMP parameters
  - Link Keys



# What can you do in BT 3.0 HS and a smartwatch

	Ubertooth	Expensive sniffer
Eavesdropping	no	Yes
Packet decryption	no	Yes (if link keys are known)
MiTM	no	Possible

Is Bluetooth secure????



System and Network  
Engineering



UNIVERSITEIT VAN AMSTERDAM

# Evaluation of the security of smartwatch communication

## Conclusion

Ubertooth useless for now on BT 3.0+HS

JustWork implementation  
Communication secured

