Evaluation of the security of smartwatch communication

Security of Systems & Networks

James Gratchoff, Harm Dermois, Florian Ecard

System and Network Engineering

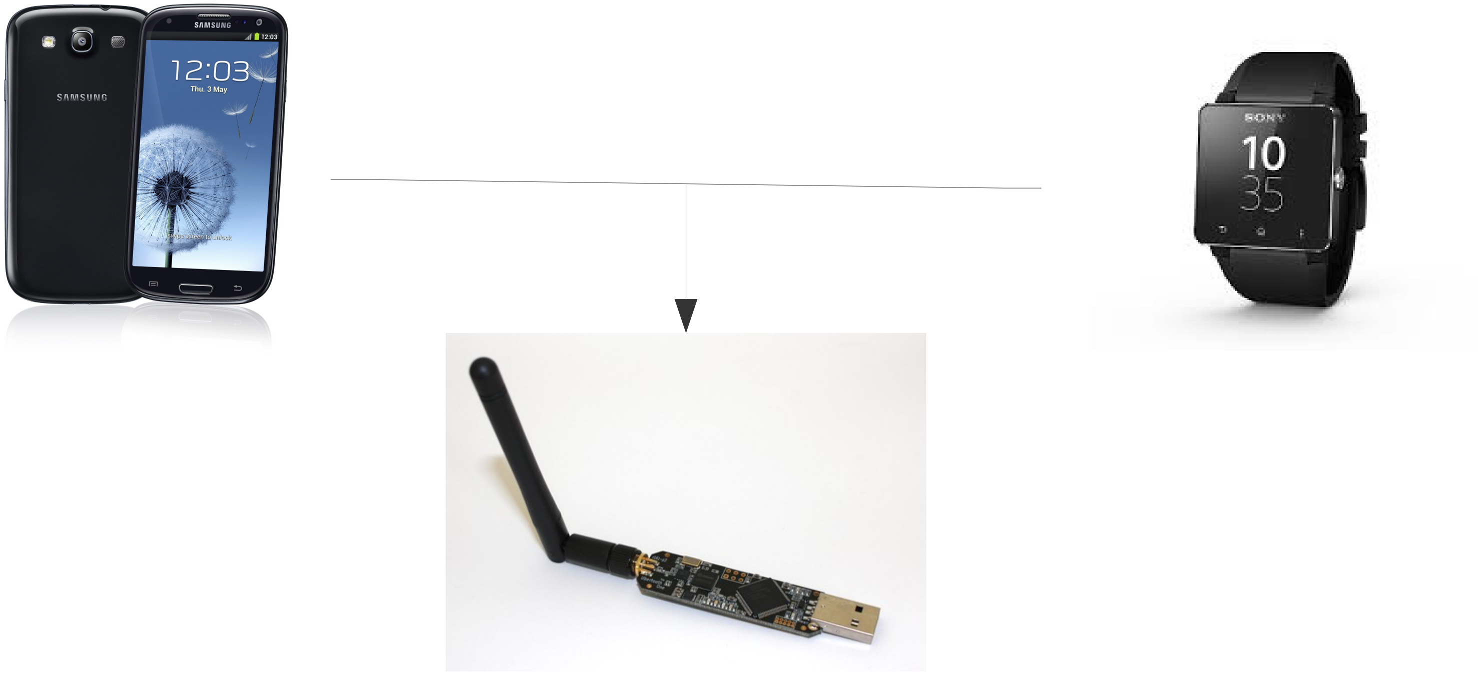
Universiteit van Amsterdam

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

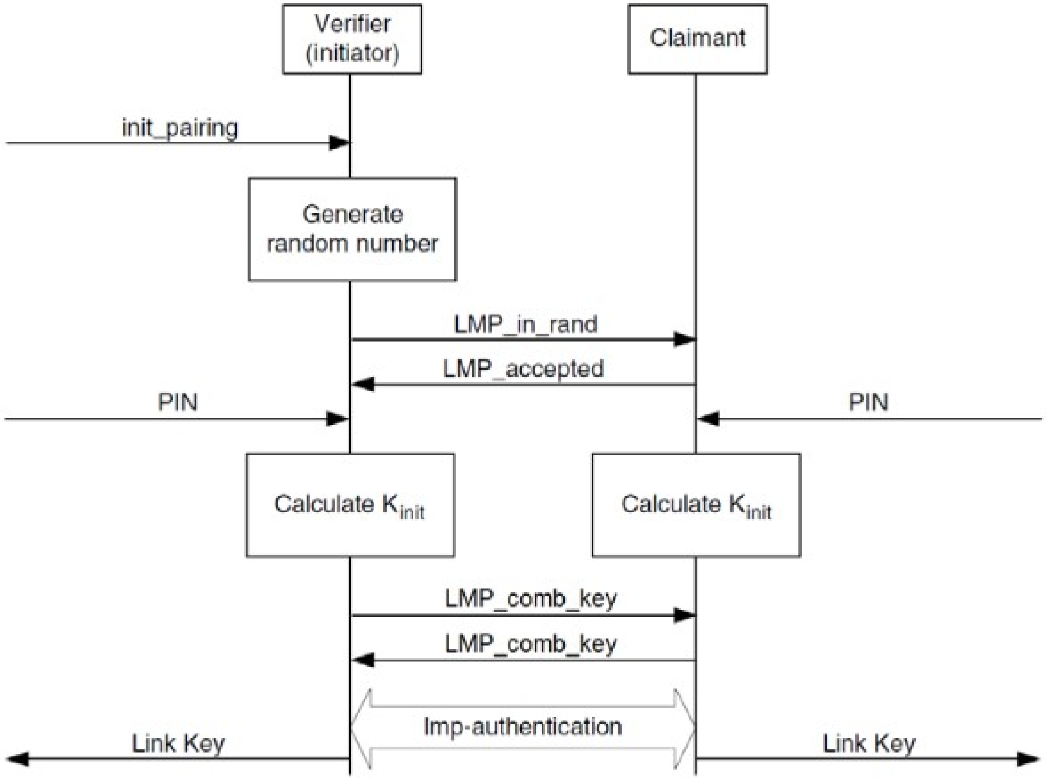


System and Network
Engineering

UNIVERSITEIT VAN AMSTERDAM

Bluetooth security and pairing process

LMP & its limitations



Bluetooth security and pairing process

SSP & MiTM protection

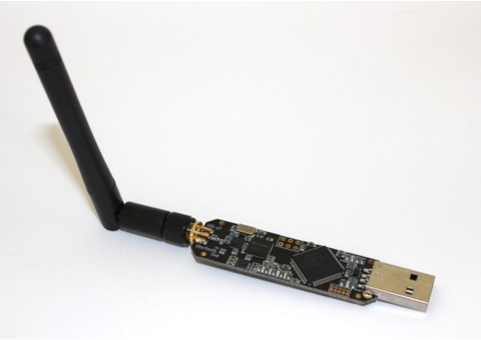
Uses Elliptic curve & DH

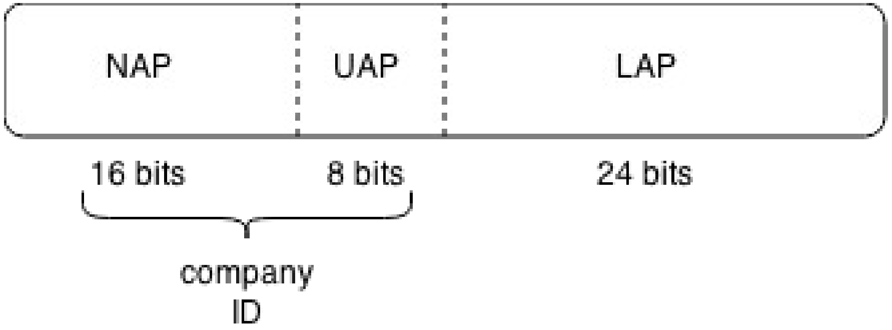
Four association models:

- Numeric comparison
- OOB
- PassKey
- JustWorks

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

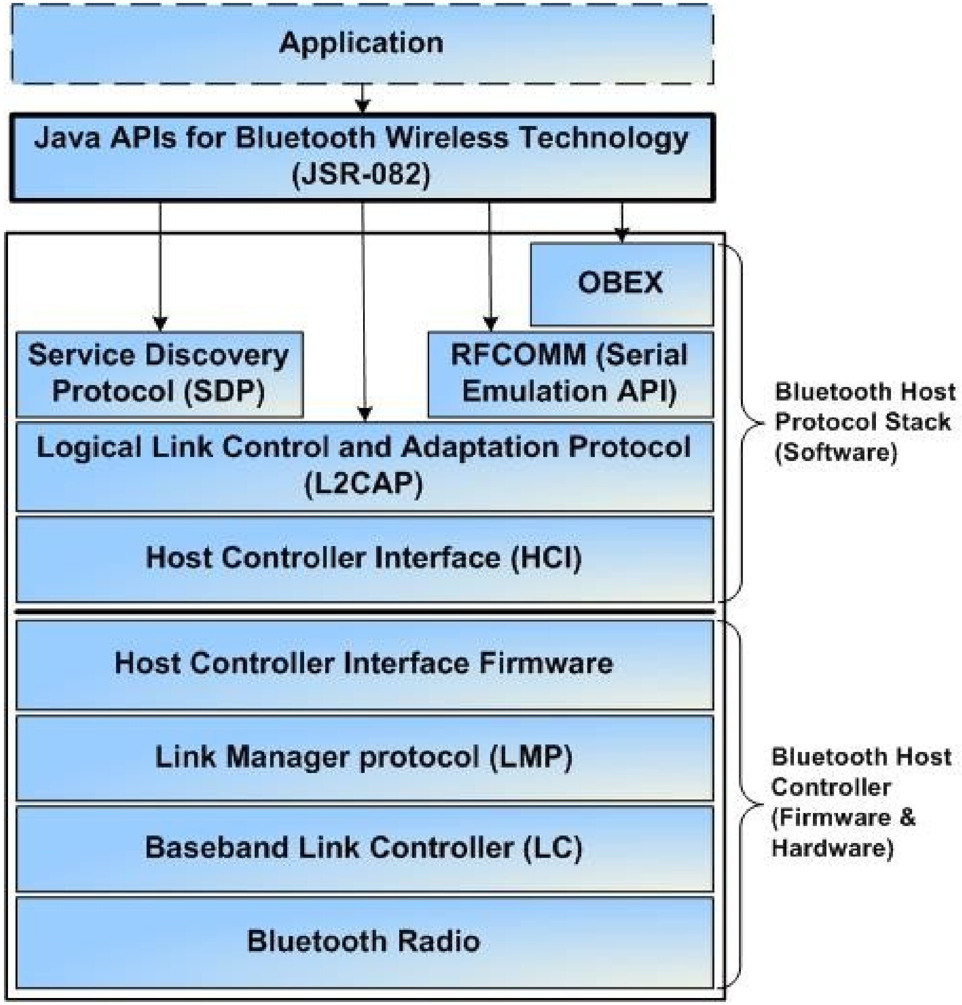
BT snoop

Most apps do not work

Traffic analysis from the Ubertooth

Only discovery
Poll and Null
Link control

Bluetooth stack


Application
Java APIs for Bluetooth Wireless Technology (JSR-082)
OBEX
Service Discovery Protocol (SDP)
RFCOMM (Serial Emulation API)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Host Controller Interface Firmware
Link Manager protocol (LMP)
Baseband Link Controller (LC)
Bluetooth Radio
Bluetooth Host Protocol Stack (Software)
Bluetooth Host Controller (Firmware & Hardware)

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????

Evaluation of the security of smartwatch communication

Conclusion

Ubertooth useless for now on BT 3.0+HS

JustWork implementation
Communication secured

System and Network Engineering

Universiteit van Amsterdam