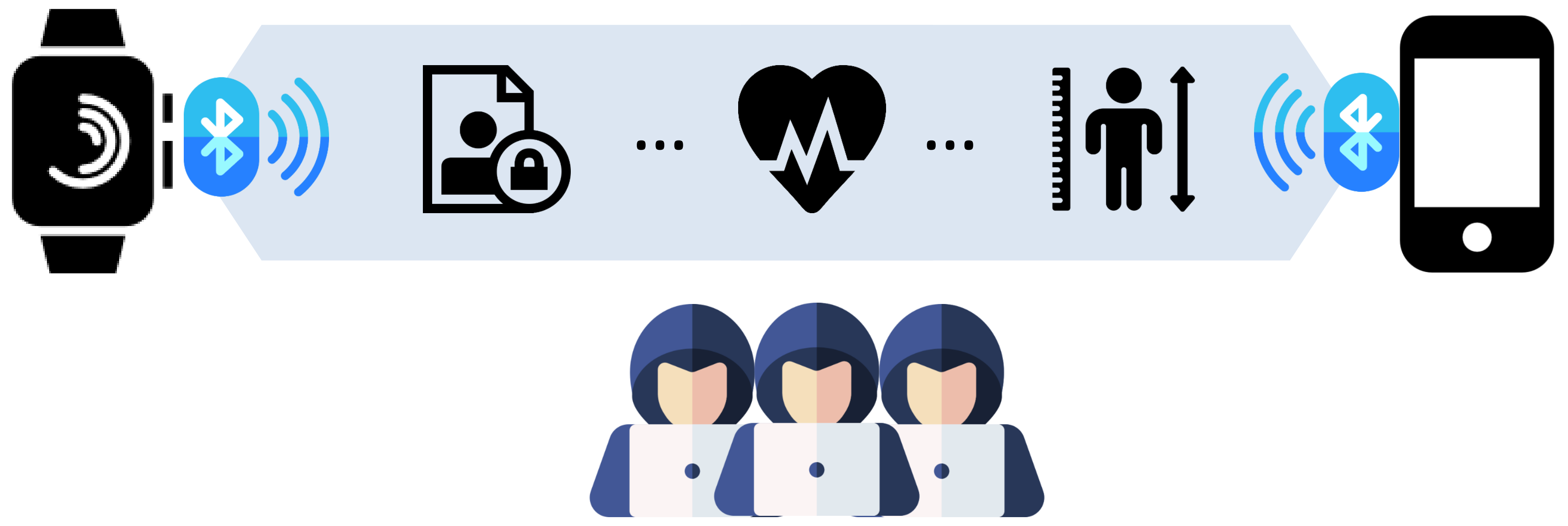
2022 - NS - 8D9-DD2 - Security Analysis of Bluetooth Low Energy in Smartwatch - Haimin Ku

CERIAS
The Center for Education and Research in Information Assurance and Security

Security Analysis of Bluetooth Low Energy in Smartwatch

Haimin Ku, Baijian Yang, Anthony Smith
Dept. Computer Information and Technology

Motivation



Problem: private-sensitive data over insecure BLE connection

Bluetooth Low Energy (BLE) v4.0

- Widely used in smartwatches
- Lightweight but vulnerable
- E.g. illegal device access, fingerprinting, and sensitive information

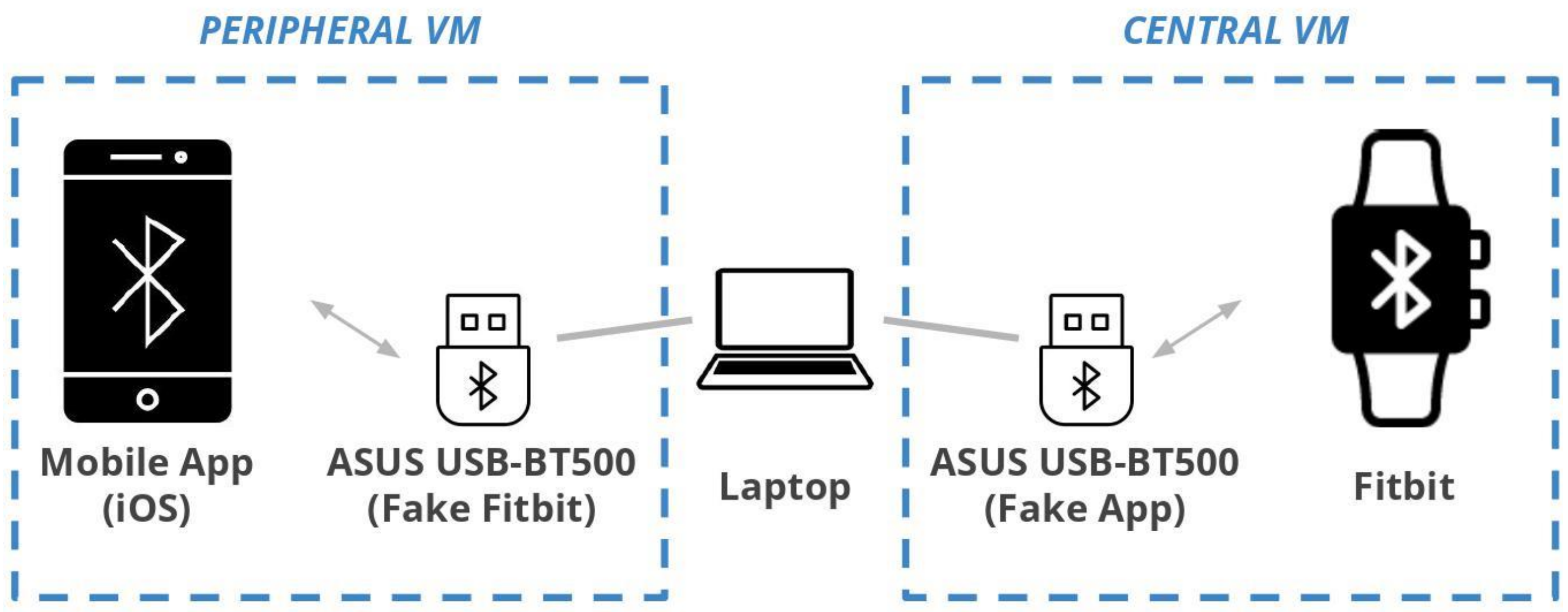
Objective: experimentally demonstrate various BLE attacks

Target device: Fibit Alta HR device

What to focus: pairing process

Why? exchange secret keys to encrypt communication channel

Man-in-the-Middle Attack



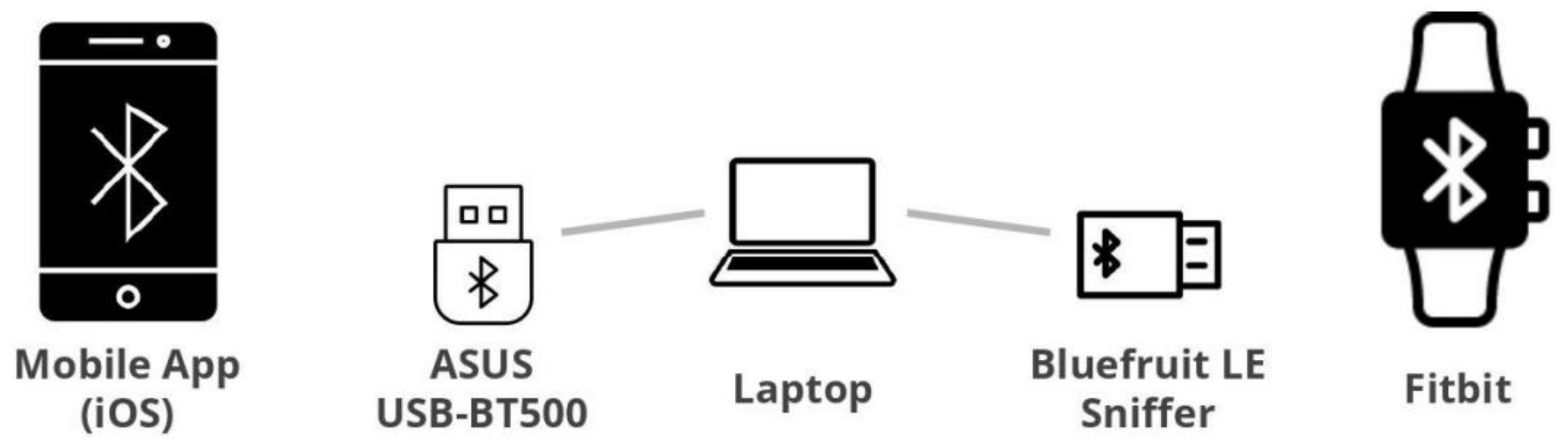
Methodology

❶ Find Fibit's MAC address by scanning
❷ Discover Fitbit's Info (services, characteristics, etc)
❸ Make a copy of Fibit using the info
❹ Trick mobile app to connect to fake Fibit
❺ Forward all data to the original Fitbit via fake app

Result: success

▪ By capturing and modifying packets from the fake connection, we replayed a synchronization with the manipulated data

Brute-force Attack



Methodology

❶ Capture packets via Wireshark
❷ Check the paring event in packets using Crackle
❸ Try paring with a random secret key
❹ Repeat ❸ until success

Result: fail

▪ Fitbit relies on its own encryption method which hinders to capture the paring event in the packet

Conclusion

Overall, Fitbit Alta HR provides a mature level of BLE security mechanism.
Nevertheless, our study demonstrates that the prior vulnerabilities on BLE v4.0 are still existing on Fibit Alta HR.
Future work: attacks on other paring methods of BLE v4.0.

PURDUE UNIVERSITY Discovery Park
CERIAS