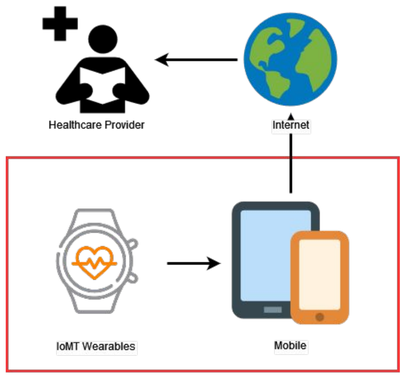
Internet of Medical Things Wearable Device Security

Jacson Ott, Trevor Hornsby, Stu Kernstock, & Matthew Chau

Problem Statement

- IoT devices are notoriously insecure.
  - Over 50% of IoT devices were vulnerable to medium or high severity attacks in 2020, according to Unit 42 [1] .
- Medical data is a high-value target for attackers.
  - AT&T Cybersecurity reported that medical data accounted for more than 43% of data breaches in 2021[2] .

Project Scope



IoMT encompasses many different sub-categories of devices.

Our research limited the scope to the following:

- IoMT wearables (watches)
- Mobile phones
- Device specific mobile applications

Devices Tested

Smart Watches

Fitbit Charge 4
Amazon Halo
Apple Watch Series 3
Popglory Smart Watch
Wyze Smart Watch

Phones

Motorola Droid XT1585
Samsung Galaxy A11
Motorola E
Apple iPhone 6

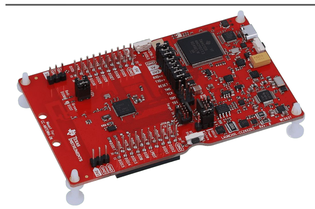
Tools Used

Several open-source tools were used during this project, some of which require special hardware:

- L2ping
- Btlejack
- Sniffle
- Wireshark
- Crackle
- Bettercap
- Spooftooph
- Jadx

**Links to tools can be found in the paper*

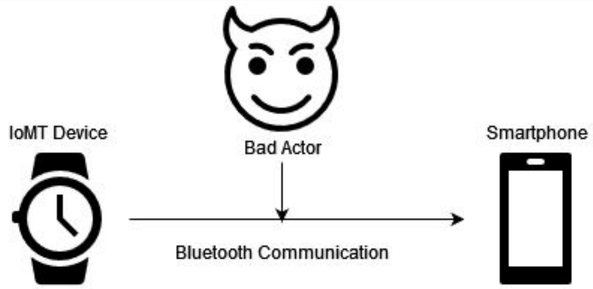
Adafruit Bluefruit LE Sniffer



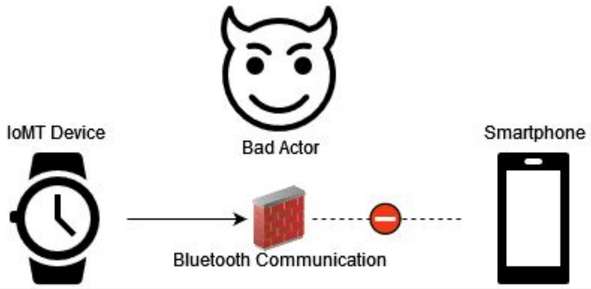
Texas Instruments LaunchPad

Attacks

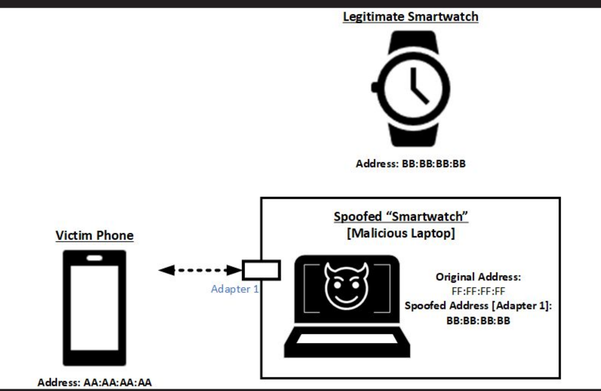
Sniffing



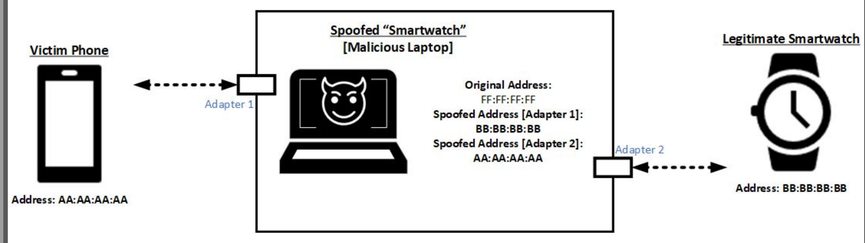
Denial of Service



Spoofing



Man in the Middle



Results Matrix

Attack/ Device	Amazon Halo	Apple Watch 3	Fitbit Charge 4	Popglory	Wyze Watch
DoS	⛔	⛔	🔒	✅	🔒
Fuzzing	⛔	⛔	⛔	⛔	⛔
Hijacking	⛔	⛔	⛔	✅	🔒
Physical	⛔	⛔	⛔	⛔	⛔
Reverse Engineering	N/A	N/A	🔒	🔒	N/A
Sniffing	⛔	⛔	🔒	✅	✅
Spoofing	🔒	⛔	🔒	✅	⛔

Findings

- **Sniffing attacks** permitted viewing of sensitive health information, such as heart rate and blood pressure in real time.
- **Spoofed connections** forged between a malicious laptop and victim phone was conducted with minimal effort.
- **Hijacking attacks** demonstrated the ability to fully disrupt the confidentiality, availability, and integrity of wearable devices and can be launched against active connections.
- **DoS attacks** were found to have limited success through hardware limitations and improved protocol functionality.
- **Not all devices** implemented important security features such as encryption.

Recommendations & Future Work

Recommendations

For Developers/ Manufacturers:

1. Implement encryption for connections.
2. Use Bluetooth 5.0 or higher.
3. Implement random MAC addresses.

For users:

1. Avoid unnecessary pairing and unpairing.
2. Opt for reputable brands.

Continued research

1. Sending false SMS messages to hijacked devices.
2. Fuzzing attacks using BluetoothStackSmasher.
3. Man in the Middle attacks utilizing rfcomm for socket forwarding.
4. Random MAC addresses.
5. Malicious Android applications.

Scan the QR code to view our paper or visit:
https://www.overleaf.com/read/xgkgjqdnkzcd

[1] https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[2] https://cybersecurity.att.com/blogs/security-essentials/securing-iomt-devices-to-protect-the-future-of-healthcare-from-rising-attacks