BLUETOOTH SECURITY/ATTACKS

Team 8: Marjia, Doyle and Attalla
What is Bluetooth?

- Bluetooth is a wireless method of transferring information from one device to another.
- Bluetooth is one of the most secure wireless communication protocols.
- It exchanges data between two devices in the form of packet.
- A packet consists of Access Code, Header and Payload.
Bluetooth Connection

- Bluetooth technology is used primarily to establish wireless personal area networks (WPAN).
- It must establish that this is a device that has connected before or to set up a new connection.
- It requires approval for new connections.
- A Bluetooth connection is usually secure from hacking from outside devices not already part of your network.
More Bluetooth devices
Benefits of Bluetooth Technology

- Cable replacement.
- Ease of file sharing.
- Wireless synchronization.
- Internet connectivity.
Bluetooth Vulnerabilities:

- After first use, unit key becomes public
- Can lead to eavesdropping
- Pin management
- Encryption keystream repetition
- Secure storage of link keys
- Repeated authentication attempts
Some headsets have security vulnerabilities:

- It is easier to hack
- Easy to listen in on or record conversation
- A hacker could then gain personal info to use against you
Bluetooth is a very accurate tracking signal!

- Many apps have access to monitor location
- Using bluetooth on a device
- When bluetooth is turned off, it stops transmitting, but still recognizes signals near your device.
PIN THEFT ATTACK

- Full control of device
  - Steal, alter or delete data from memory or external storage
- Pins are used during pairing
- After PIN exchange, pairing is done in 3 steps
  - Key init generation
  - Link Key generation
  - Authentication
  - Encryption via Link Key (optional)
- Attacker can eavesdrop on pairing
- All that’s left is PIN which is 1-8 bytes
  - brute force

---

Fig. 1. LMP-Pairing and LMP-Authentication [9, vol.4, p.223-224]

PIN CRACKING ATTACK (ONLINE)

- Attacker does not have to eavesdrop on pairing in order to crack PIN
- Generate Link Key based on a guessed PIN
- If response does not match challenge, the wrong PIN was guessed
- Attacker starts over with another PIN and different Address

Prevention and Pairing Guide

- Turn bluetooth off
- Undiscoverable
- Use a strong PIN and update regularly
- Pair in short range and in private
- Avoid unknown pairing
- Monitor paired list

Key Negotiation Attack

- Key Negotiation of Bluetooth (KNOB) attack, **affects all Bluetooth versions**!

- The specification of encryption is **negotiated** by the paired parties
  - This process is **not authenticated** or checked for integrity!

- Bluetooth is used worldwide but different countries have different cryptographic export controls or privacy laws, so the **key size is a negotiable parameter** in this process.

- The key size (N) is the entropy of the key, Bluetooth minimum is 1 byte!
  - 1 byte of entropy == 256 candidate keys! (easy to bruteforce!)
Alice (controller)  Charlie (attacker)  Bob (controller)

\[
\begin{array}{c}
A & C & B \\
\text{LMP: AU\_RAND} & \text{LMP: AU\_RAND} \\
\text{LMP: SRES} & \text{LMP: SRES} \\
\text{LMP encryption mode req: 1} & \text{LMP encryption mode req: 1} \\
\text{LMP accept} & \text{LMP accept} \\
\text{LMP } K'_C \text{ entropy: 16} & \text{LMP } K'_C \text{ entropy: 1} \\
\text{LMP } K'_C \text{ entropy: 1} & \text{LMP accept} \\
\text{LMP accept} & \text{LMP start encryption: EN\_RAND} \\
\text{LMP start encryption: EN\_RAND} & \text{LMP accept} \\
\text{LMP accept} & \text{LMP accept} \\
\end{array}
\]

Encryption key $K'_C$ has 1 byte of entropy

**Capabilities**

- Attacker can sniff traffic
- Attacker can inject traffic
- Can take control of either device!
- Affected **ALL** smartphones and major bluetooth devices as of 2018!

**Discovery**

- Discovered in 2018
- Confidently released to industry (Bluetooth Group)
- Patches released and public disclosure in August 2019
THREE KEY QUESTIONS

1. How is bluetooth an accurate tracking signal even when it is turned off?

2. Does an attacker have to be eavesdropping in order to crack a bluetooth pin?

3. What does the key negotiation procedure lack that makes it vulnerable to KNOB attack?