Bluetooth Attacks

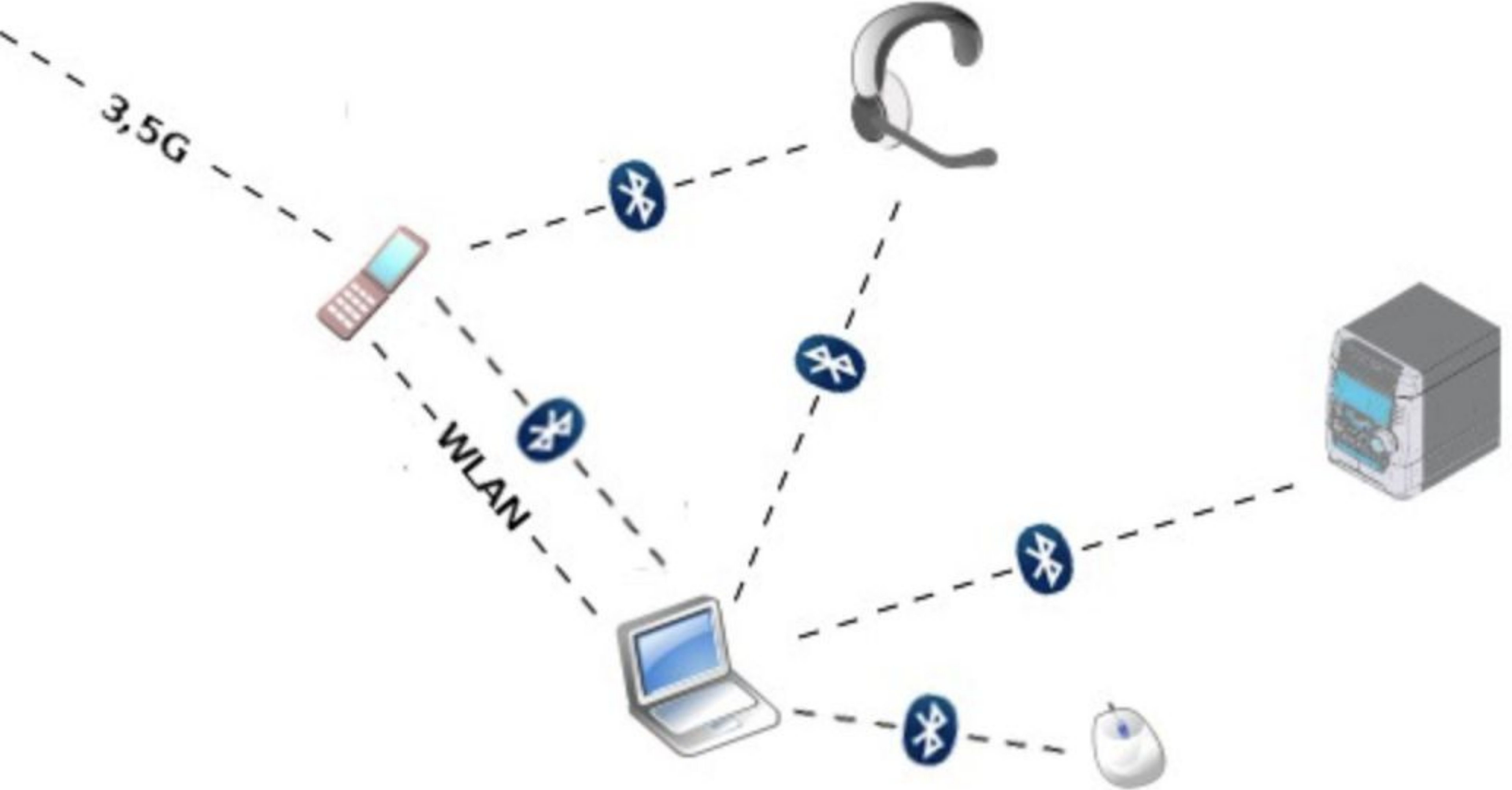
Hello!

Ammar Halawani, Milad Jafarieh, Amanda D’Errico

- Overview of Bluetooth technology
- Provide real-life examples of recent Bluetooth exploits.
- Discuss several recommended measures to secure Bluetooth communication.

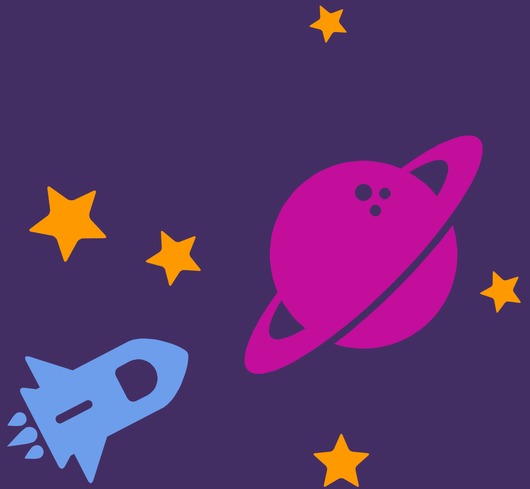
Overview of Bluetooth technology

- Was invented in 1994 at Ericsson.
- In 1998, they developed and promoted the open industry standard for Bluetooth technology
- Bluetooth enables, low power communication between devices that has a range 0.5-1 m to 100 m
- Ability to transmit both voice and data simultaneously
- To avoid interferences with the 2.4 GHz radio frequency spectrum, Bluetooth used technology called spread spectrum


3,5G
WLAN

Important Terms For the next slides

- ***Piconet:*** a spontaneous, ad hoc network that enables two or more Bluetooth devices to communicate with one another.
- ***Link Key:*** is the secret key that both devices generate the first time they communicate.
- ***RFCOMM Protocol:*** Radio frequency communication is simple set of transport protocols, made on top of the L2CAP Protocol.
- ***L2CAP:*** The Logical Link Control Adaptation Protocol.
- ***BD_ADDR:*** Every Bluetooth device has a unique 48-bit address used for identification, known as the BD_ADDR.



Bluetooth Attacks

Most common bluetooth attacks

Different Stages of Attacks

Before The Pairing Process

- During Formation of Piconets.
- When Link Keys are being generated.

After Devices Are Paired

- Based on the information the attackers collect after pairing

Before Devices Are Paired

MAC Spoofing Attack

Before encryption.

During formation of piconet.

While link keys are generating.

Attacker acts like other user.

PIN Cracking Attack

While pairing and authenticating.

By a frequency sniffer tool.

Using a brute-force algorithm to find PIN.

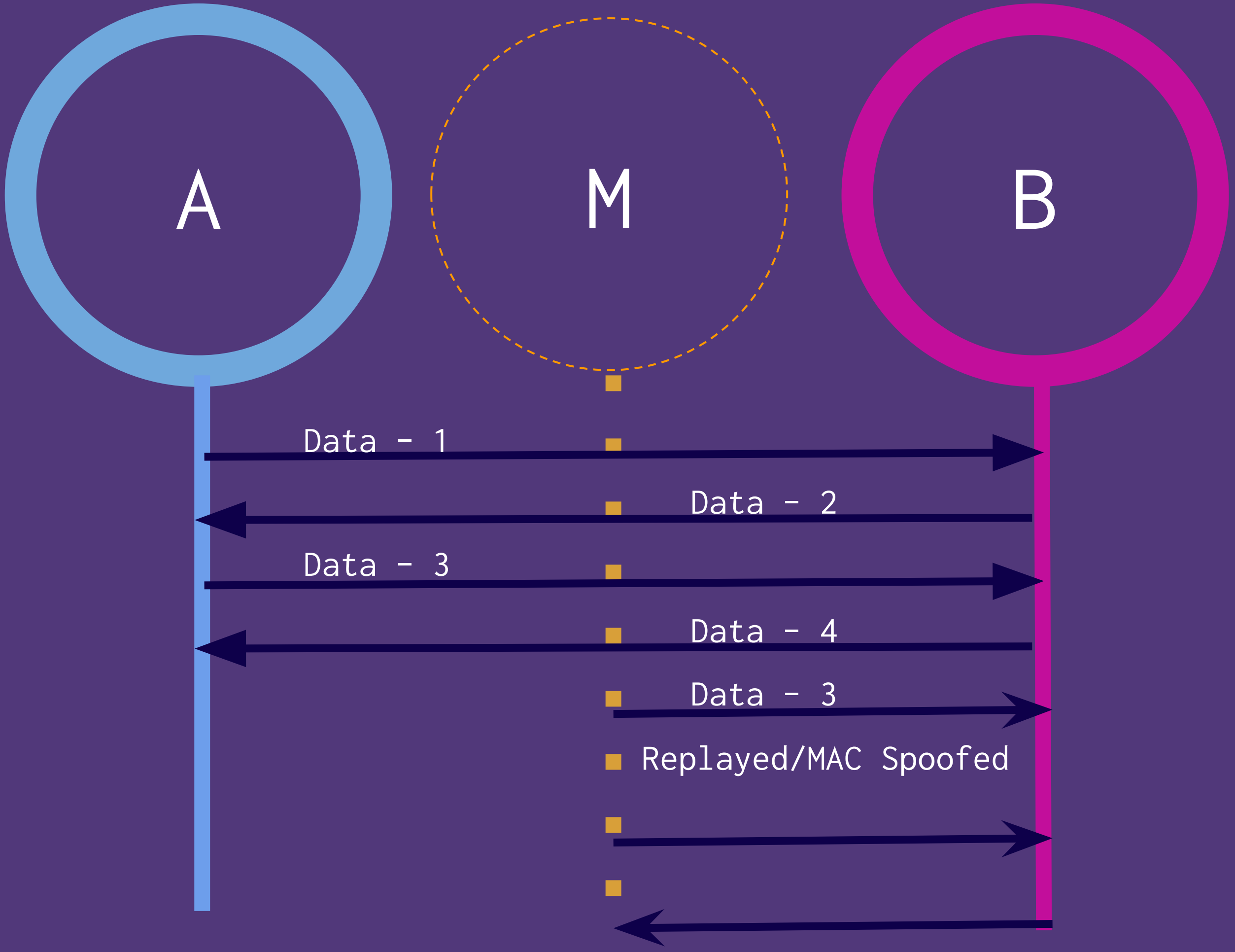
(E22)

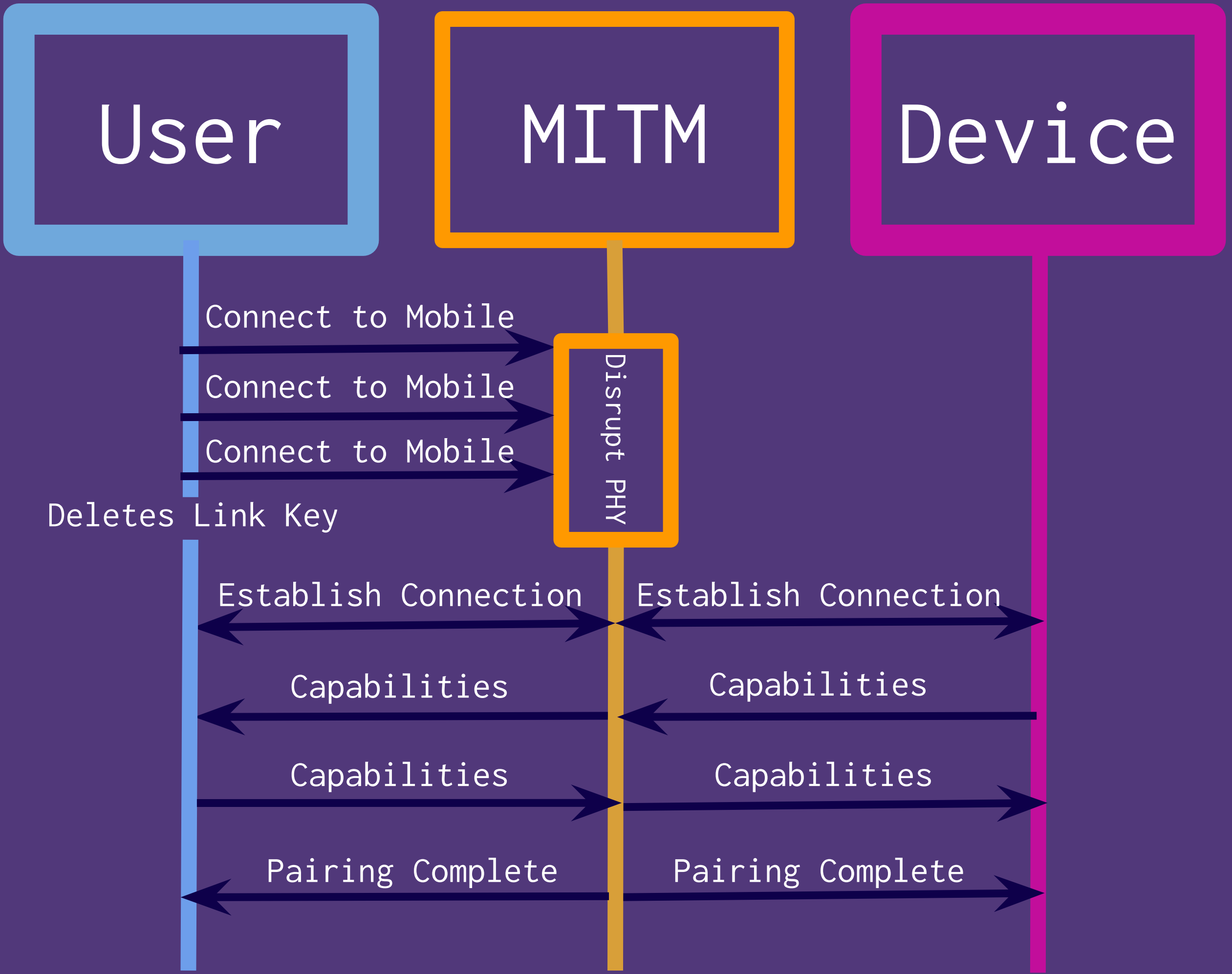
Man-in-the-Middle Attack

Whole Devices are trying to pair.

Authentication without the shared secret keys by relayed messages.

Devices are paired to the attacker.


A
M
B
Data - 1
Data - 2
Data - 3
Data - 4
Data - 3
Replayed/MAC Spoofed


User
MITM
Device
Connect to Mobile
Connect to Mobile
Connect to Mobile
Disrupt PHY
Deletes Link Key
Establish Connection
Establish Connection
Capabilities
Capabilities
Capabilities
Capabilities
Pairing Complete
Pairing Complete

Before Devices Are Paired

BlueJacking Attack

By sending unwanted messages to device to trick the user into using an access code.

Gives access to target's files.

Prepares device for other attacks.

BlueSnarfing Attack

Stealing mobile phone's memory data.

OBEX FTP.

By pairing to user's device.

BlueBugging Attack

Connecting to the device without owner knowing.

Happens in RFCOMM Protocol.

Attacker takes control of the device by accessing AT commands.

Information get stolen, access to setting and services granted to attacker.

Before Devices Are Paired

BlueBump Attack

When there is weakness in handling link-keys.

Force user to accept a business card.

Keeping the connection active after pairing.

Attacker can pair with device later by link-key regeneration request.

BlueDump Attack

Spoofing BD_ADDR of a device to connect with other.

Targeted device deletes its link key and goes to pairing mode.

BluePrinting Attack

When BD_ADDR of the device is known.

Using some known information to gain additional information.

Before Devices Are Paired

BlueOver Attack

Auditing tool that is used to determine if a device is vulnerable to attacks.

Can be used to initiate BlueBugging attack.

BlueBorne Attack

By taking advantage of a stack buffer overflow weakness.

Attacker can hijack the Bluetooth connection.

Require MAC and Bluetooth addresses.

Fuzzing Attack

Attacker tries to make a device behave abnormal.

By sending non-standard and malformed data packets to a device.

After Devices Are Paired

Off-Line PIN Recovery Attack

The Attacker tries to intercept several values.

bsD

Then finding a PIN by using brute-force.

Brute-Force BD_ADDR Attack

Scanning last three bytes of BD_ADDR

Reflection/Relay Attack

Attacker impersonates a device.

Authenticating the connection by relaying/reflecting the device information.

After Devices Are Paired

Backdoor Attack

Creating a trusted pairing.

User cannot see the attacker in the paired devices list.

Attacker has access to device resources and services.

BD_ADDR is required for this attack.

DoS/DDoS Attack

Attacker intend to crash the network or restart the system.

Target the Physical layer in the protocol stack or above Physical layer.

BD_ADDR duplication, BlueSmack, BlueChop, Battery Exhaustion,Big NAK, L2CAP guaranteed service.

Worm Attacks

Trojan files or malicious software spreading through Bluetooth devices.

In symbian mobile phones.

Before/After Devices Are Paired

Bluesmack Attack

DoS attack.

Similar to Ping of Death.

On IP-based devices.

Sending 600 bytes pings and L2CAP echo requests to Bluetooth devices.

Causing input buffer overflow.

MultiBlue Attack

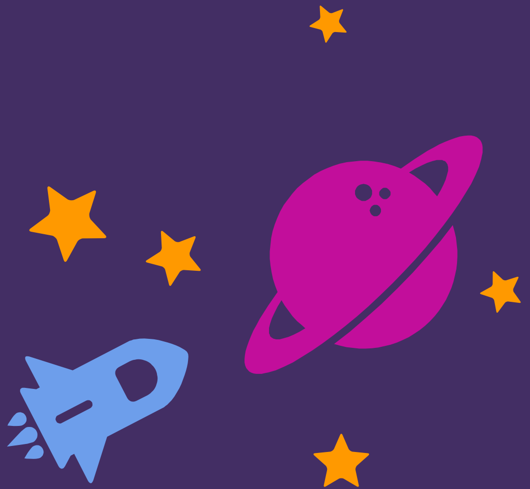
When attacker has access to the target device.

The MultiBlue dongle.

Sending targeted devices send pairing request.

Target devices send pre-shared keys.

Attacker controls the device.



Bluetooth Attacks

Recommended Measures for Bluetooth Security

Bluetooth Risk Mitigations

- Awareness about security practices
- Base the link keys on combination keys
- Use link encryption for all data transmissions
- Ensure all links are encryption-enable
- Require mutual authentication on network devices
- Encrypting broadcasts
- Use maximum encryption key size
- Set a minimum encryption key size
- Use highest security level - Bluetooth Security Mode 3

Thanks!

Any questions?

Credits / References

Cope, P.; Campbell, J.; Hayajneh, T. An Investigation of Bluetooth Security Vulnerabilities. In Proceedings of the 7th IEEE Annual Computing and Communication Workshop and Conference (IEEE CCWC 2017), Las Vegas, NV, USA, 9-11 January 2017

Nateq Be-Nazir Ibn, M.; Tarique, M. Bluetooth security threats and solutions: A survey. Int. J. Distrib. Parallel Syst. 2012, 3, 127.

Saravanan, K.; Vijayanand, L.; Negesh, R.K. A Novel Bluetooth Man-In-The-Middle Attack Based on SSP using OOB Association model. arXiv, 2012, arxiv:1203.4649.

Moreno, A.; Okamoto, E. BlueSnarf Revisited: OBEX FTP Service Directory Traversal. Available online:

https://link.springer.com/content/pdf/10.1007%2F978-3-642-23041-7_16.pdf (accessed on April 2019).

Becker, A. Bluetooth Security & Hacks; Seminar ITS Ruhr-Universitat Bochum SS2007; Ruhr University of Bochum: Bochum, Germany, 2007; Available online: https://gsyc.urjc.es/~anto/ubicuos2/bluetooth_

security_and_hacks.pdf (accessed on 1 April 2019).

Trifinite: BlueBump. Available online: https://trifinite.org/trifinite_stuff_bluebump.html (accessed on 1 April 2019).

BlueDump. Available online: https://trifinite.org/trifinite_stuff_bluedump.htm (accessed on 1 April 2019).

Credits / References

Bisikian, C. An overview of the Bluetooth wireless technology. IEEE Commun. Mag. 2001, 39, 86-94. [CrossRef].

Cope, P.; Campbell, J.; Hayajneh, T. An Investigation of Bluetooth Security Vulnerabilities. In Proceedings of the 7th IEEE Annual Computing and Communication Workshop and Conference (IEEE CCWC 2017), Las Vegas, NV, USA, 9-11 January 2017.

Red Hat CVE-2017-1000251. Available online: https://access.redhat.com/security/cve/cve-2017-1000251 (accessed on 1 April 2019).

The Attack Vector “BlueBorne” Exposes Almost Every Connected Device. Available online: https://www.armis.com/blueborne/ (accessed on 1 April 2019).

Tsira, V.; Nandi, G. Bluetooth technology: Security issues and its prevention. Int. J. Comput. Appl. Technol. 2014, 5, 1833-1837.

Haataja, K. Security Threats and Countermeasures in Bluetooth-Enabled Systems. Kuopio University Publications H. Business and Information Technology 13. 2009. Page 75. Available online: http://epublications.uef.fi/pub/urn_isbn_978-951-27-0111-7/urn_isbn_978-951-27-0111-7.pdf (accessed on 1 April 2019).

Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O. Internet of Things (IoT): Taxonomy of Security Attacks. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11-12 August 2016.

Trifinite: BluePrinting. Available online: https://trifinite.org/trifinite_stuff_bluesmack.html (accessed on 1 April 2019).

Using MultiBlue to Control Any Mobile Device. Available online: https://null-byte.wonderhowto.com/how-to/hack-bluetooth-part-2-using-multiblue-control-any-mobile-device-0164377/ (accessed on 1 April 2019).