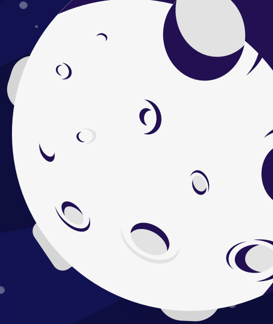


Bluetooth Security/ Attacks

Team 8: Marjia, Doyle and Attalla

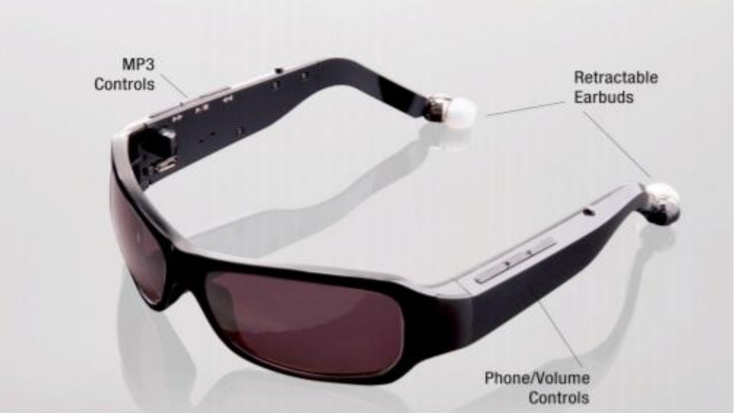
What is Bluetooth?

- 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:

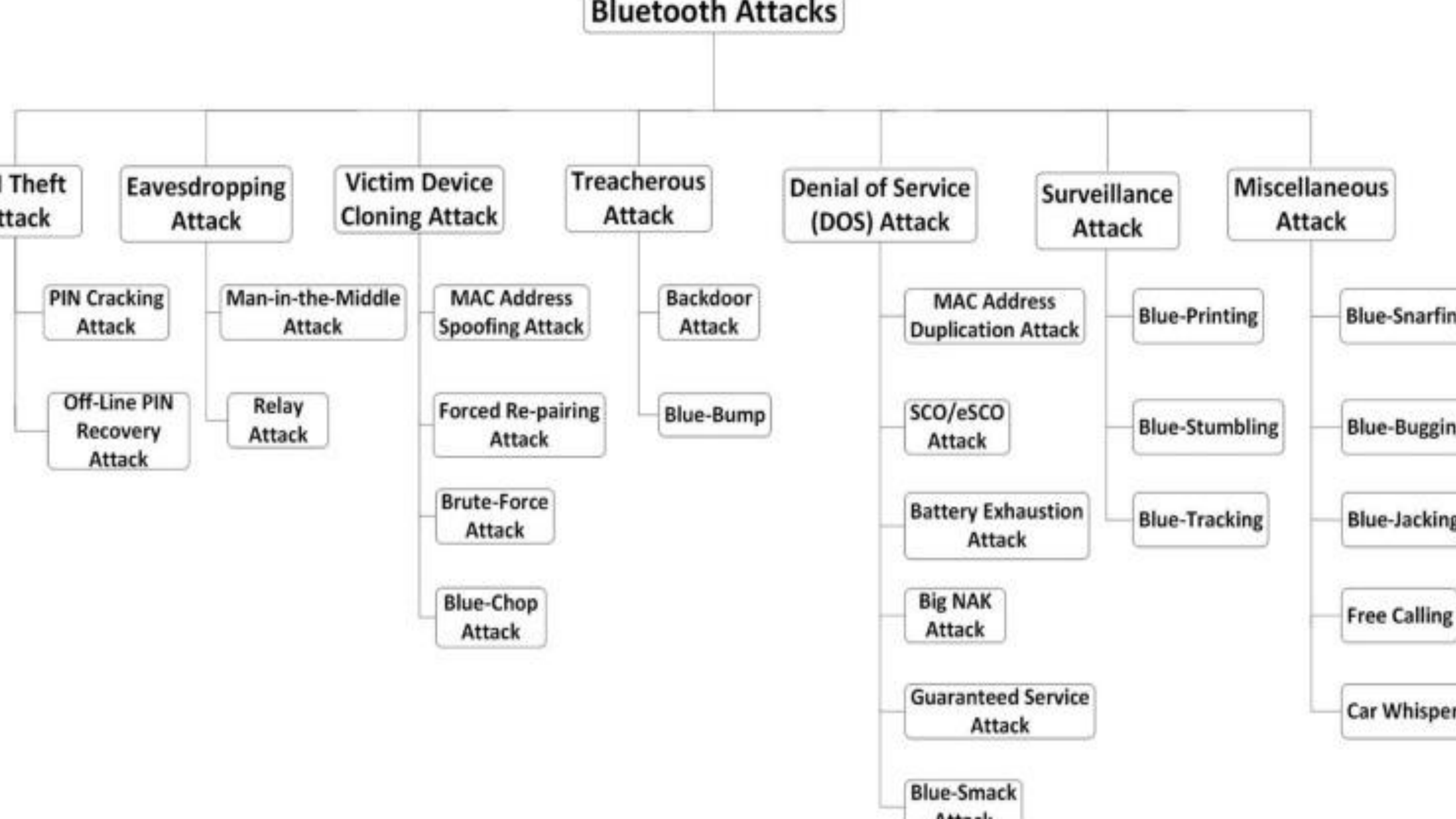
- After first use, unit key becomes public
- Can lead to eavesdropping
- Pin management
- Encryption keystream repetition
- Secure storage of link keys
- Repeated authentication attempts

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.


Bluetooth Attacks
l Theft ttack
PIN Cracking Attack
Off-Line PIN Recovery Attack
Eavesdropping Attack
Man-in-the-Middle Attack
Relay Attack
Victim Device Cloning Attack
MAC Address Spoofing Attack
Forced Re-pairing Attack
Brute-Force Attack
Blue-Chop Attack
Treacherous Attack
Backdoor Attack
Blue-Bump
Denial of Service (DOS) Attack
MAC Address Duplication Attack
SCO/eSCO Attack
Battery Exhaustion Attack
Big NAK Attack
Guaranteed Service Attack
Blue-Smack Attack
Surveillance Attack
Blue-Printing
Blue-Stumbling
Blue-Tracking
Miscellaneous Attack
Blue-Snarfin
Blue-Buggin
Blue-Jacking
Free Calling
Car Whisper

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 step
  - 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

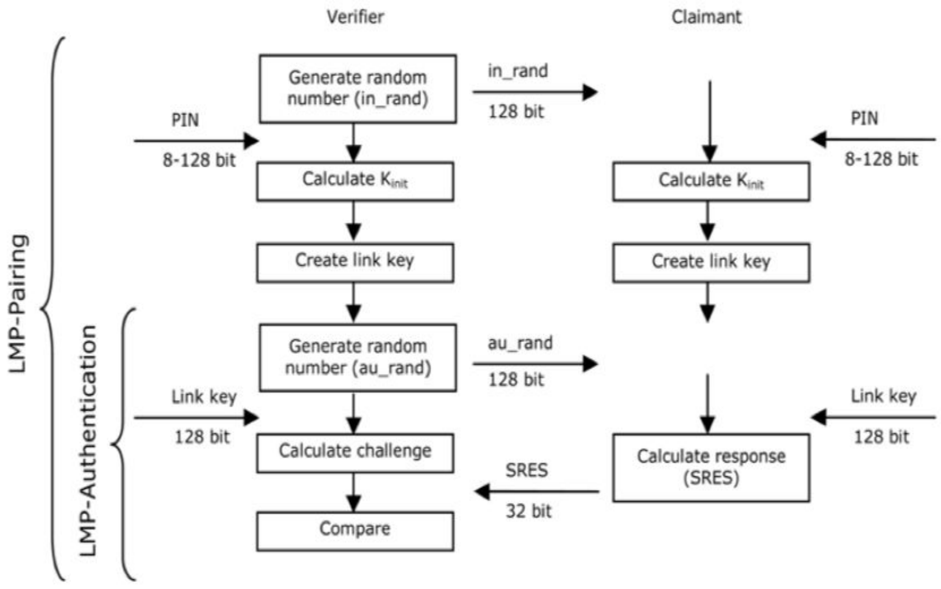


Fig. 1. LMP-Pairing and LMP-Authentication [9, vol.4, p.223-224]

Herfurt M, Mulliner C. Bluetooth security vulnerabilities and bluetooth projects, Web page; 2005. Available from:http://trifinite.org/trifinite_stuff.html. [Accessed November 11]

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

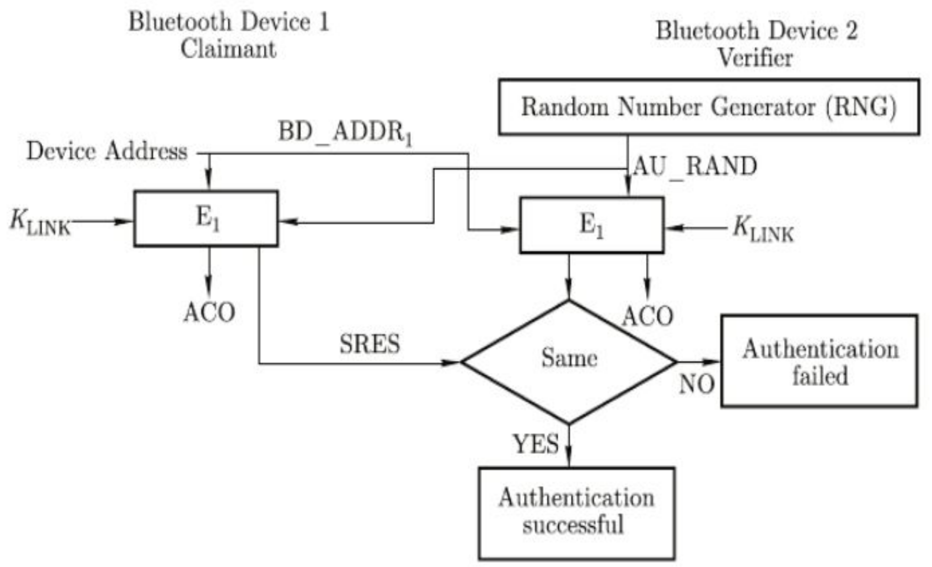


Fig. 5.3 Bluetooth authentication process.

Shaked Y, Wool A. Cracking the Bluetooth PIN, in 3rd international conference on mobile systems, applications, and services. New York, USA: ACM, pp. 39–50, 2005.

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

Shaikh, Shahriar, Hassan. Security Threats in Bluetooth Technology. ScienceDirect.com [retrieved_2019-11-10]

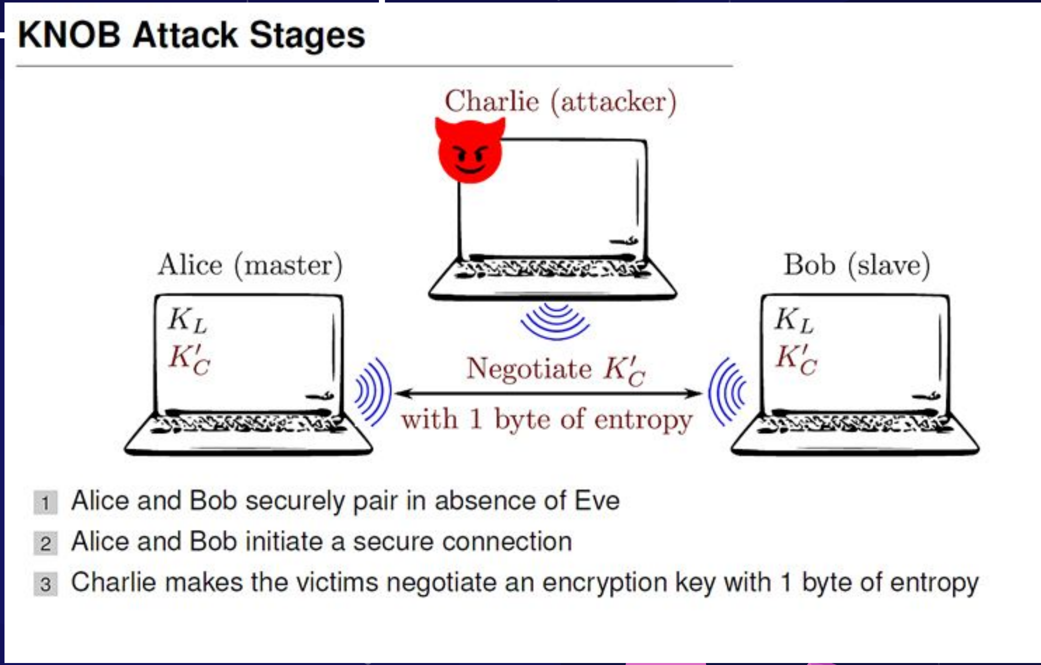
Key Negotiation Attack

- 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!

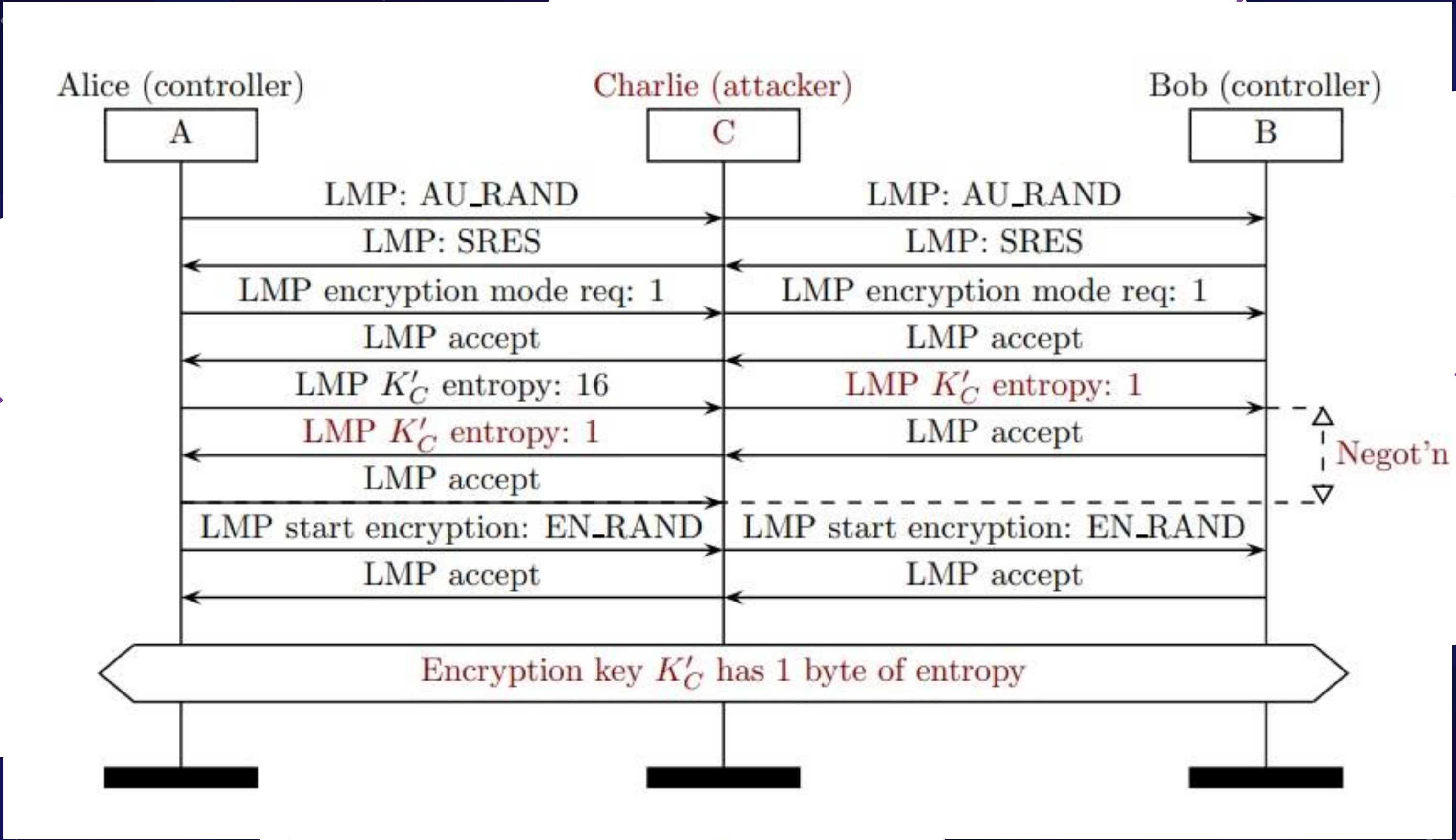
- Bluetooth is used worldwide but different countries have different cryptographic export controls or privacy laws, so the **key size is a negotiable parameter** in this process.

- 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!)



KNOB Attack Stages

1. Alice and Bob securely pair in absence of Eve
2. Alice and Bob initiate a secure connection
3. Charlie makes the victims negotiate an encryption key with 1 byte of entropy



Antonioli, Daniele. "Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR." *Https://Francozappa.github.io/Publication/Knob/Slides.pdf*, Singapore University of Technology and Design, 2019, francozappa.github.io/publication/knob/slides.pdf.

Capabilities

Attacker can sniff traffic

Attacker can inject traffic

Can take control of either device!

Affected **<u>ALL</u>** smartphones and major bluetooth devices as of 2018!

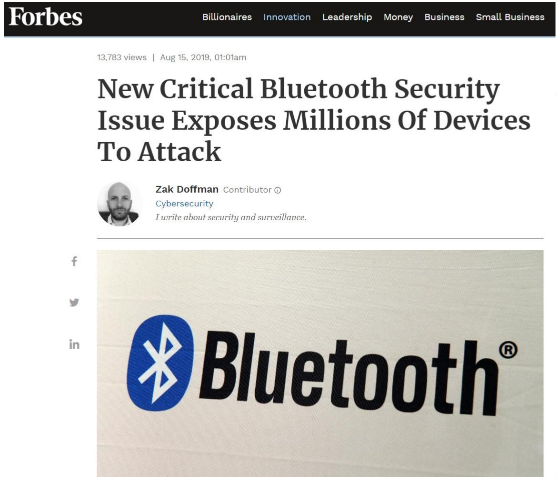
Discovery

Discovered in 2018

Confidentially released to industry (Bluetooth Group)

Patches released and public disclosure in August 2019

IMPACT



13,783 views | Aug 15, 2019, 01:01am

New Critical Bluetooth Security Issue Exposes Millions Of Devices To Attack

Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.

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?