Module 7 Bluetooth Technology and Security

News

- https://www.csoonline.com/article/1291144/magic-keyboard-vulnerability-allows-takeover-of-ios-android-linux-and-macos-devices.html

Bluetooth

Bluetooth Reading

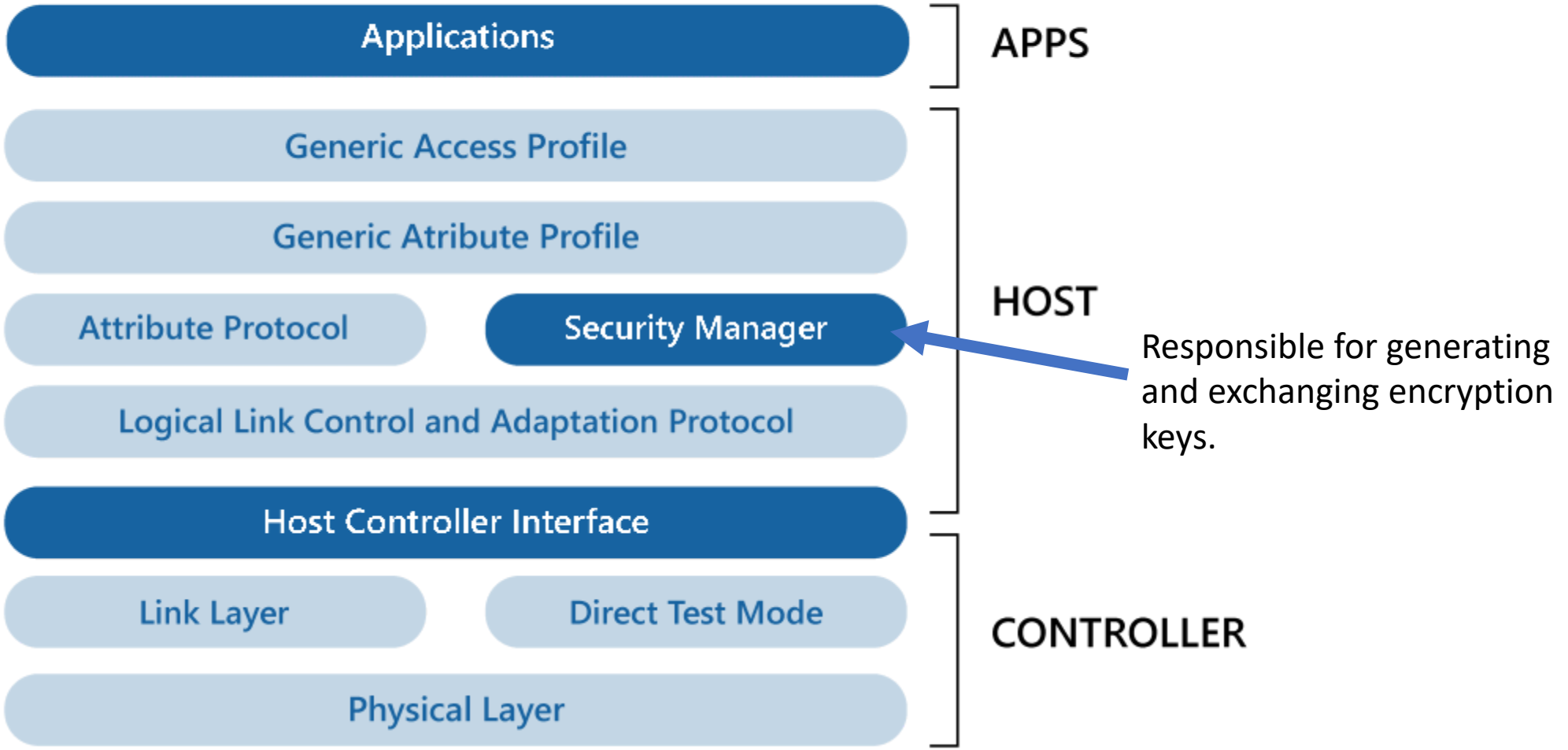
- Summary of NIST Guidelines

Bluetooth Types

- **Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR)** is typically used for relatively short-range, continuous wireless connection. “Classic Bluetooth”. Primary option for most speakers and headsets. Bluetooth 5.2 offers a high speed LE option.

- **Bluetooth Low Energy (LE)** is designed to use short bursts of longer-range radio connection, making it ideal for Internet of Things (IoT) applications that don’t require continuous connection.

Bluetooth Low Energy Architecture

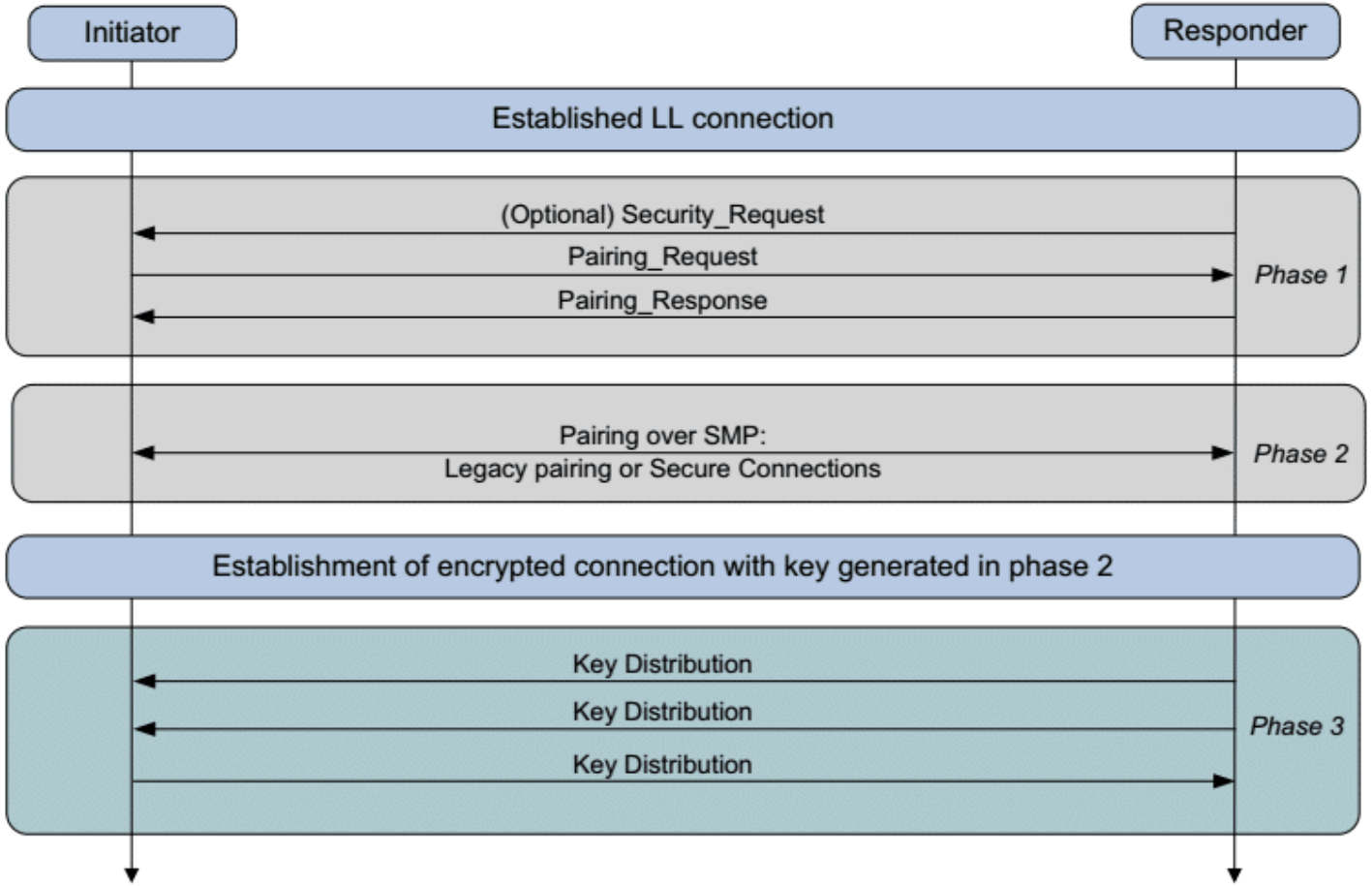


Bluetooth Security

Five basic security services are specified in the Bluetooth standard:

- **Authentication:** Verifies the Bluetooth device address
- **Confidentiality:** Prevents eavesdropping
- **Authorization:** Ensures a device is authorized to use a service before being permitted to do so
- **Message Integrity:** verifying that a message sent between two Bluetooth devices has not been altered in transit
- **Pairing/Bonding:** creating one or more shared secret keys and the storing of these keys for use in subsequent connections to form a trusted device pair. Bonding is persistent and does not require re-pairing on a new connection
- Does not address other security services such as audit and non-repudiation

Bluetooth Security Phases



Pairing
Exchange features and security requirements

Bonding - optional

Bluetooth Service Types

- Two Bluetooth service security types:
  - **Trusted:** Trusted device has full access to all services of another trusting device
  - **Untrusted:** Untrusted devices do not have an established relationship and can reach only restricted services

Bluetooth Pairing

- **Numeric Comparison**. Both devices display the same six-digit value on their respective screens or LCD displays, and you make sure they match and hit or click the appropriate button on each device. This is not to prevent a man-in-the-middle (MITM) attack, but rather to identify the devices to each other.

- **Just Works**. Obviously, not all devices have a display, such as headphones or a speaker. Therefore, the Just Works method is probably the most popular one. Technically, it is the same as Numeric Comparison, but the six-digit value is set to all zeros. While Numeric Comparison requires some on-the-fly math if you are performing a MITM attack, there is no MITM protection with Just Works.

Bluetooth Pairing Continued

- **Passkey Entry**. With Passkey Entry, a six-digit value is displayed on one device, and this is entered into the other device.
- **Out Of Band (OOB)**. A communication method outside of the Bluetooth communication channel is not used, but the information is still secured. The Apple Watch is a good example of this workflow. During the Apple Watch pairing method, a swirling display of dots is displayed on the watch face, and you point the pairing iPhone's camera at the watch face. Another example is using Near Field Communication (NFC) between NFC-capable headphones and a pairing phone.

Bluetooth1 Pairing pcap

Bluetooth Security Modes

These modes dictate when a Bluetooth device initiates security, not whether it supports security features.

- **Security Mode 1**—Devices that use this mode are designed and produced with no security features, making them vulnerable to attack.
- **Security Mode 2**—A service level-enforced security mode, security procedures may be initiated after link establishment but before logical channel establishment.
- **Security Mode 3**—This mode requires that Bluetooth devices initiate security before the physical network connection can be established. In Security Mode 3, authentication and encryption are mandatory for all connections.
- **Security Mode 4**—Like Mode 2, it is a service-level security mode that uses Secure Simple Pairing (SSP), a secure method of pairing or connecting Bluetooth devices.

Bluetooth Mode 4 Service Levels

- For Security Mode 4, Bluetooth specifications call out five separate service levels:
  - **Service Level 4 –** Requires MITM protection and encryption using 128-bit equivalent strength for link and encryption keys; user interaction is acceptable.
  - **Service Level 3:** Requires man-in-the-middle protection and encryption, and preferably user interaction
  - **Service Level 2:** Requires encryption only
  - **Service Level 1:** Does not require encryption; user interaction is not necessary
  - **Service Level 0:** Requires neither man-in-the-middle protection and encryption, nor user interaction

Bluetooth Security Concerns

Bluejacking

- Came about through the misuse of a Bluetooth feature whereby a mobile phone could exchange a "business card" or messages with another phone in the vicinity
- Used in Asia by storekeepers in malls, for example, for marketing and advertising
- Bluetooth devices needed to peer before communication
- Passersby didn't know with whom his or her device was peering
- After spammer's initial message was accepted, spammer's Bluetooth device ID was added to trusted contacts
- Relatively harmless

Bluesnarfing

- A technique whereby an attacker gains access to unauthorized information on a Bluetooth-enabled device such as a mobile phone
- Attacker can then access contacts, calendar, e-mails, and text messages
- Victim's phone must have Bluetooth enabled and be in discoverable mode
- Bluetooth devices must also pair
- Bluesnarfing uses a get request to pull information from the victim's device

Bluebugging

- Enables an attacker to commandeer entire handset
- Requires trusted device status
- Establishes a connection by tricking victim's phone into believing the attacker device to be a Bluetooth headset
- Then attacker can control just about every function of the phone via AT command codes
  - Attacker can listen in on conversations (hence the name **bluebugging**)

Car Whisperer

- Car Whisperer is a software tool developed by European security researchers that exploits the use of a standard (non-random) passkey in hands-free Bluetooth car kits installed in automobiles.
- The Car Whisperer software allows an attacker to send to or receive audio from the car kit. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop) from the microphone in the car.

Relay Attack

- One device near the person's phone
- One device near the target device
- A relay is performed at the link layer
- Demonstrated to unlock Teslas
- https://www.youtube.com/watch?v=5mdU4ksOc2w

Denial of Service

- Like other wireless technologies, Bluetooth is susceptible to DoS attacks. Impacts include making a device's Bluetooth interface unusable and draining the device's battery. These types of attacks are not significant and, because of the proximity required for Bluetooth use, can usually be easily averted by simply moving out of range.

Fuzzing Attacks

- Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. If a device's operation is slowed or stopped by these attacks, a serious vulnerability potentially exists in the protocol stack.

Pairing Eavesdropping

- PIN/Legacy Pairing (Bluetooth 2.0 and earlier) and low energy Legacy Pairing are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s) given sufficient time, which allows trusted device impersonation and active/passive data decryption.

Secure Simple Pairing Attacks

- A number of techniques can force a remote device to use Just Works SSP and then exploit its lack of MITM protection (e.g., the attack device claims that it has no input/output capabilities). Further, fixed passkeys could allow an attacker to perform MITM attacks as well.

Bluetooth Vulnerabilities

- https://www.armis.com/blueborne/
  - Issues in the standard Bluetooth stack
- Short-distance worm
- SweynTooth project
- https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/

Bluetooth Privacy

- Older versions of Bluetooth exposed information that could identify and track someone
- Newer versions use randomized address to prevent identification

Is Bluetooth Vulnerable?

- Bluetooth presents a trade-off between convenience and security
- Bluetooth vulnerabilities:
  - Short PINs used during pairing
  - Users pairing devices in public
  - User convenience
- What are the risks?

Bluetooth Security Measures Individuals

- Install security patches and updates
- Make your Bluetooth device not discoverable
  - Both iPhone and Android are only discoverable while you are in settings, or if an app requests discovery.
  - It's possible for an app to set discovery on for long term
- Don't share sensitive information via Bluetooth
- Don't accept connections from unknown sources
- Don't pair in public
- Unpair unused devices
- Turn off Bluetooth when not in use

Bluetooth Security Measures for Organizations

- The first line of defense is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth-enabled devices.
- Organizations using Bluetooth should establish and document security policies that address the use of Bluetooth-enabled devices and users' responsibilities.
- https://www.nist.gov/publications/guide-bluetooth-security-2 Page 54
- Bluetooth Security Assessment Methodology: https://www.tarlogic.com/news/bsam-bluetooth-security-assessment/

Bluetooth Security Measures for IoT

- Developer guidelines for securing IoT devices: https://docs.silabs.com/bluetooth/7.0.1/bluetooth-security-overview/