Android Deep Dive With Chuck Easttom

Lesson 4 Hacking Android

Hack with AndroRat

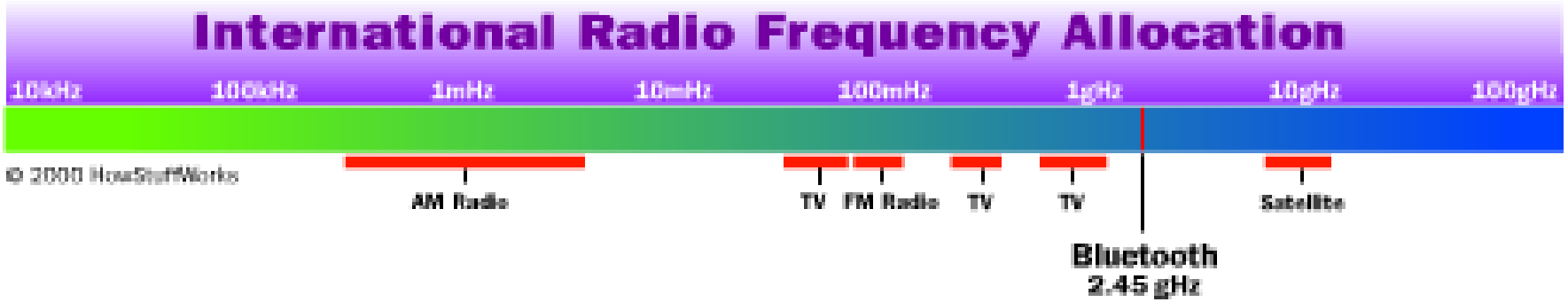
1. Go to https://www.noip.com/ to register a free domain.
2. Download DUC Updater from site, this updates your current ip to NOIP server every time you connect to the internet.
3. Login in DUC with your NOIP credentials from NOIP.com
4. : You can now extract downloaded files and run Androrat binder.exe, go to no-ip menu and login no-ip credentials
5. Go to build in same application and insert your Noip Dormain url in IP section and any port no.
6. Then press build. This creates an app with same name you inserted in apk title which you install in target phone.
7. Now run androrat.jar from androrat folder and set listing port from server menu option. Restart and wait to see target phone. Once this is visible you can then control target phone
8. Or get https://github.com/wszf/androrat and send it to the target

Clone a phone

- This is a phone you have access to and just want the data
- Step 1: Go to https://my.Copy9.com/ and clicking on "Sign Up".
- Step 2: Download the copy9 app from copy9.com and open it to install.
- Step 3: Log into your account and activate account
- Step 4: Accept (tap Allow) them and Copy9 will be installed automatically.
- Step 5: Go to my.copy9.com-> settings. Choose SMS, Calls, GPS... any information you need and then click on 'Save & Sync Now' to begin the cloning.
- Step 6: From my.Copy9.com –> Settings –> Select tab Export Data –> Choose Features or tick all Features –> Sent to email or Download

Bluetooth

Has been set aside by the ISM(Industrial ,Scientific and Medical) for exclusive use of Bluetooth wireless products



- Communicates on the 2.45 GHz frequency

Bluetooth

- **Frequency Hopping is used for interference mitigation and media access;**

- **TDD (**Test-Driven Development) **is used for separation of the transmission directions** In 3-slot or 5-slot packets

Bluetooth

- Frequency hopping (FH) is one of two basic modulation techniques used in spread spectrum signal transmission.
- It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of the unauthorized interception or jamming of telecommunications.
- It also is known as frequency- hopping code division multiple access (FH-CDMA).
- Bluetooth uses a technique called spread-spectrum frequency hopping.

Bluetooth

Version	Bandwidth/Range
3.0	25 Mbps; 10 meters (33 ft)
4.0	25 Mbps; 60 meters (200 ft)
5.0	50 Mbps; 240 meters (800 ft)

Bluetooth Protocols

Bluetooth is designed as a layer protocol architecture. This means there are layers of protocols being used. The mandatory protocols that all Bluetooth devices have are LMP, L2CAP, and SDP.

LMP: Link Management Protocol is used to setup and control the communication link between two devices.

L2CAP: Logical Link Control and Adaptation Protocol is used for multiplexing multiple connections between two devices.

SDP: Service discovery protocol is how two devices find out what services each offers.

RFCOMM: Radio Frequency Communications, as the name implies, provides a data stream. In this case, it is a virtual serial data stream.

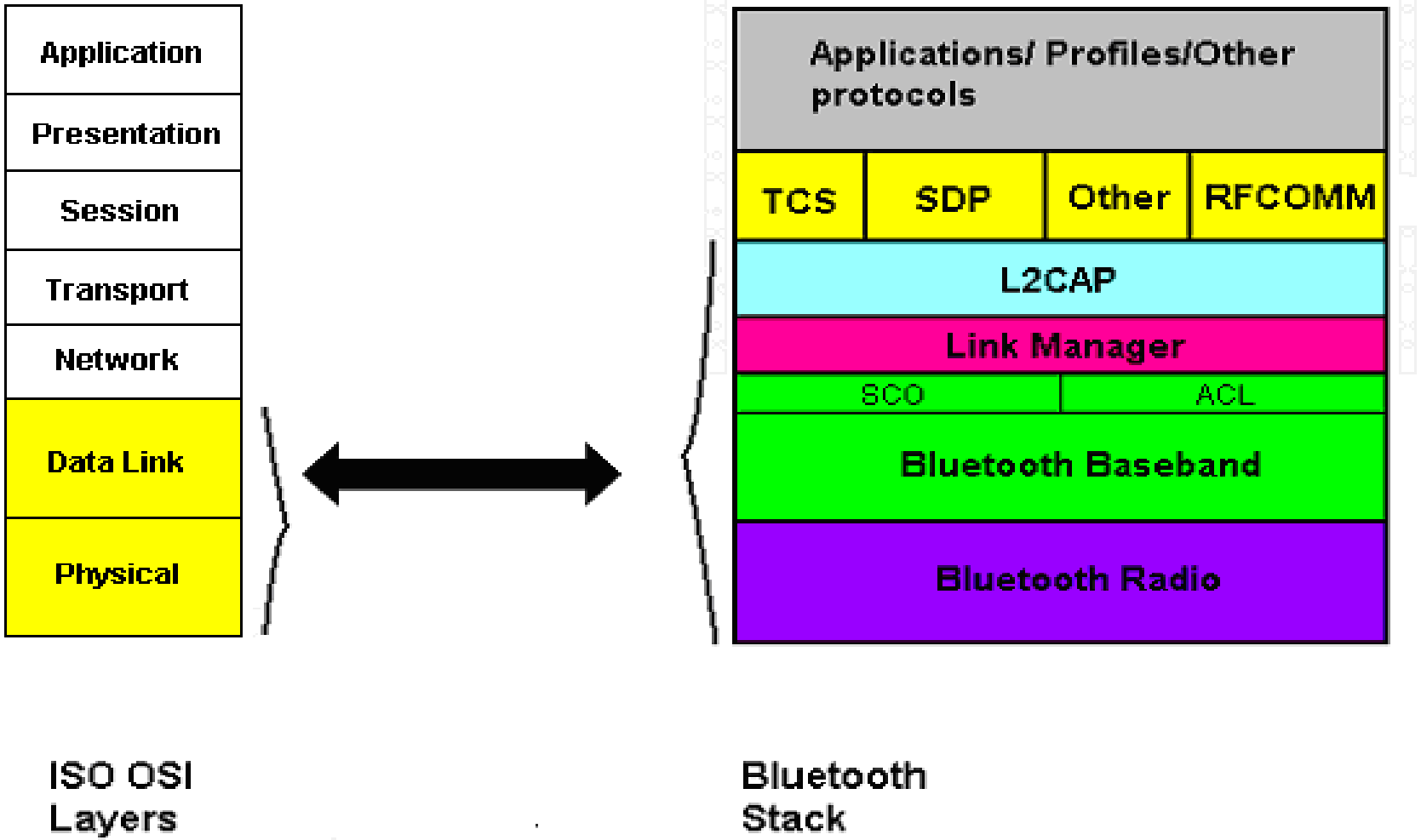
BNEP: Bluetooth Network Encapsulation Protocol is used to transfer some other protocol over the L2CAP channel. It is encapsulating the other protocol.

Bluetooth Protocols

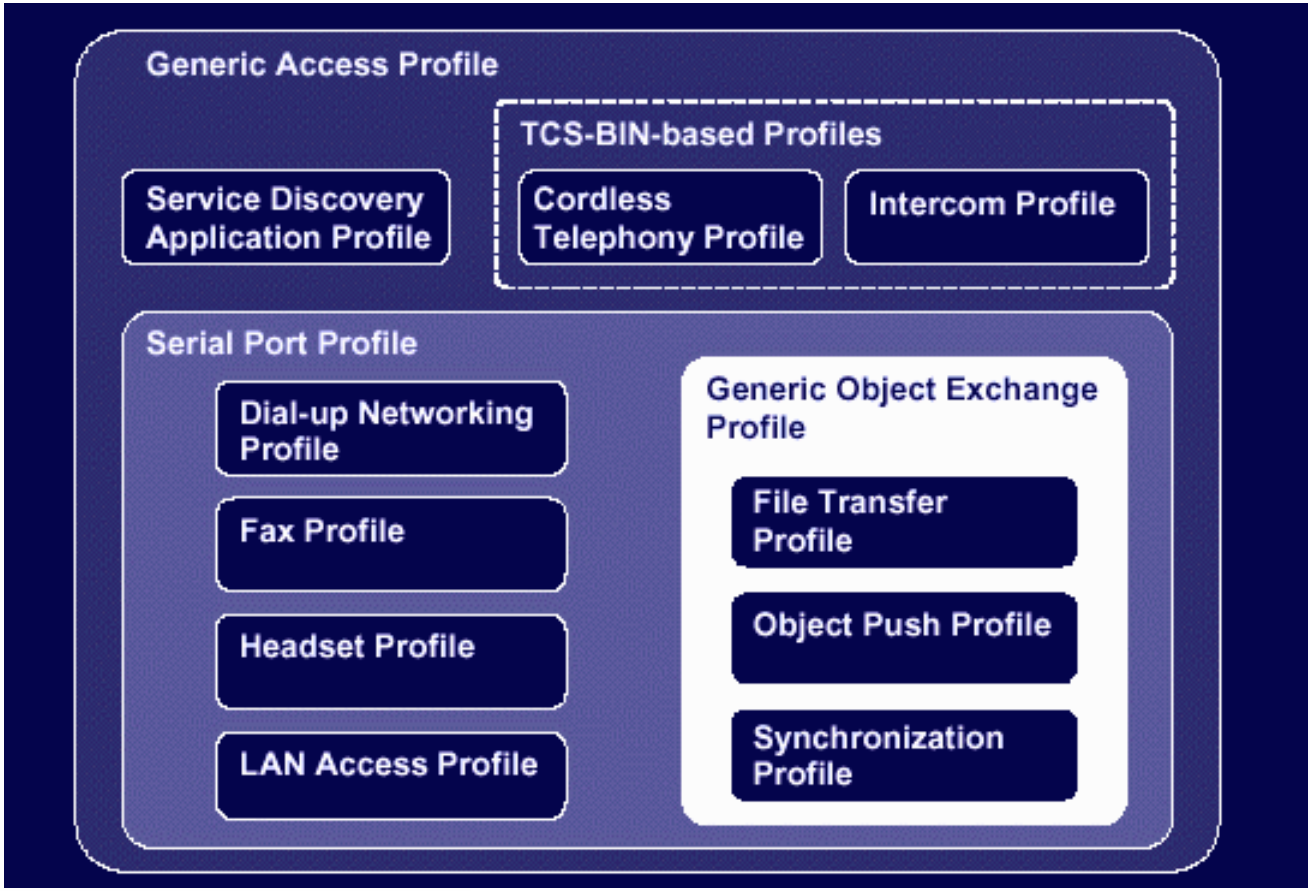
AVCTP: The Audio/Video Distribution Transport Protocol is used to transfer audio vidsual control commands over the L2CAP channel.

HCI: Host Controller Interface refers to any standardized communication between the host stack (i.e. the operating system) and the controller (the actual Bluetooth circuit).

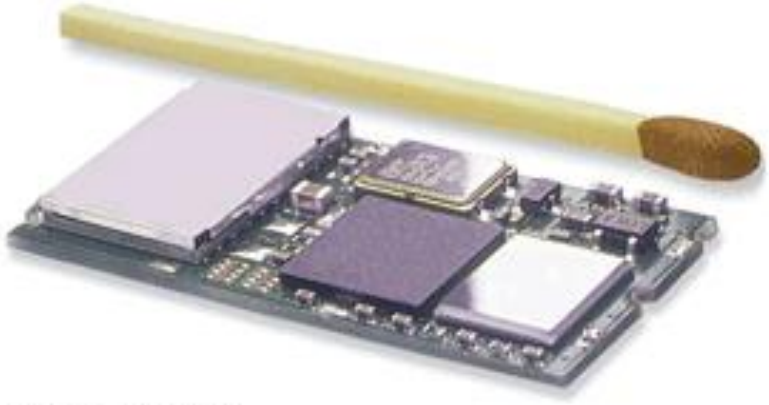
OBEX: Object Exchange it facilitates the transfer of binary objects between devices. It was originally designed for infrared, but is now used by Bluetooth. This is used in accessing phonebooks, printing, and other functions. It uses RFCOMM for communication.


Application
Presentation
Session
Transport
Network
Data Link
Physical
Applications/ Profiles/Other protocols
TCS
SDP
Other
RFCOMM
L2CAP
Link Manager
SCO
ACL
Bluetooth Baseband
Bluetooth Radio
ISO OSI Layers
Bluetooth Stack

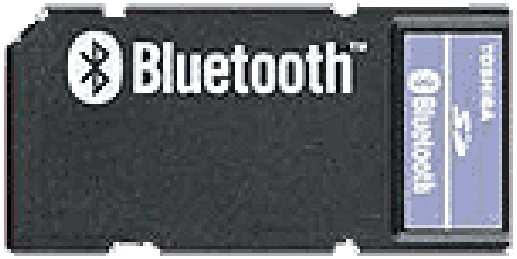
Bluetooth


Generic Access Profile
TCS-BIN-based Profiles
Service Discovery Application Profile
Cordless Telephony Profile
Intercom Profile
Serial Port Profile
Dial-up Networking Profile
Fax Profile
Headset Profile
LAN Access Profile
Generic Object Exchange Profile
File Transfer Profile
Object Push Profile
Synchronization Profile

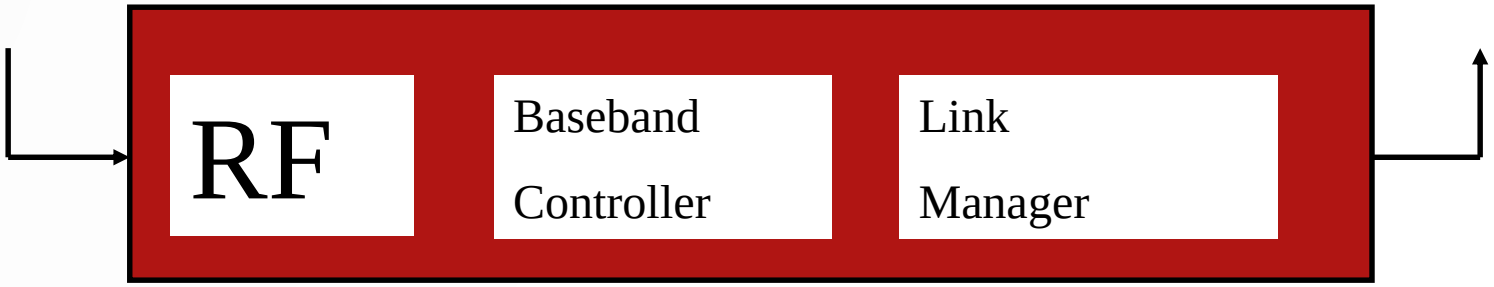
Bluetooth



Puce Bluetooth

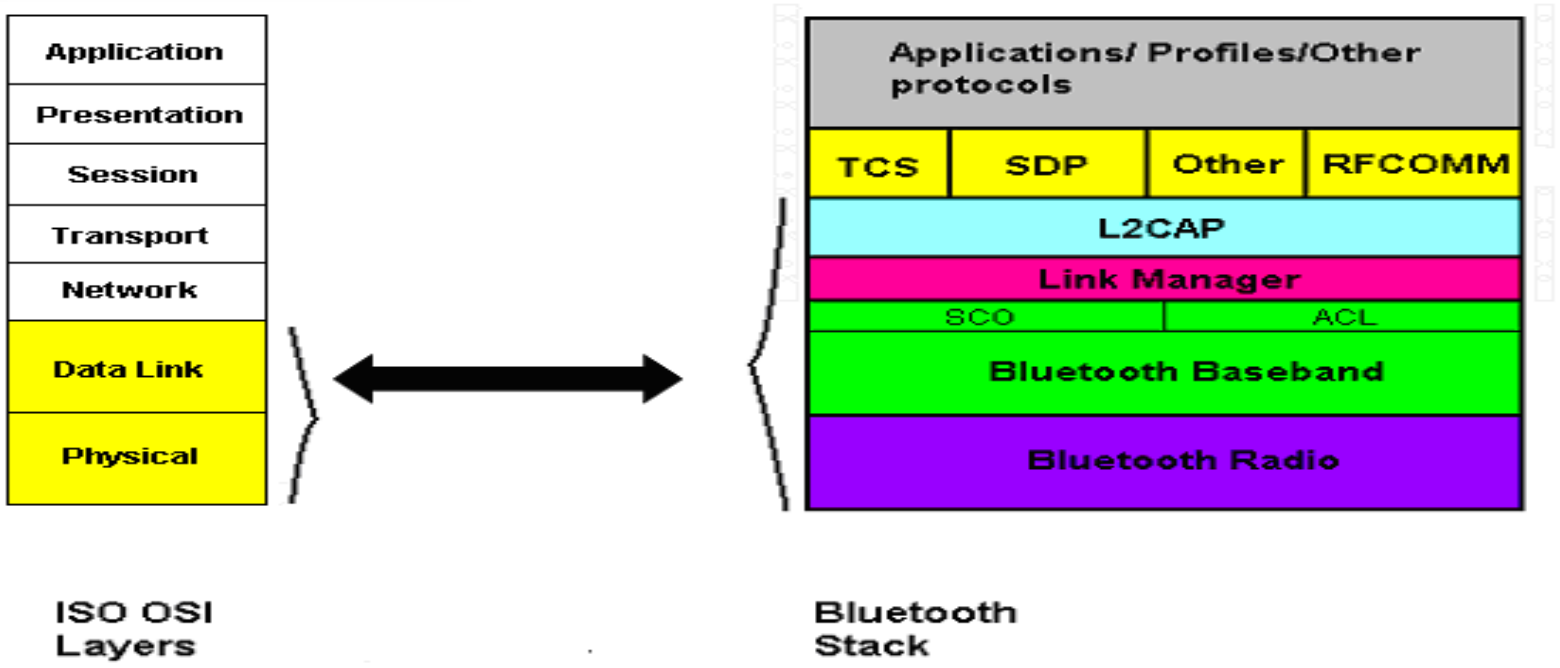


Bluetooth Chip



Bluetooth

- Bluetooth specifications are divided into two:
  - Core Specifications
    This bluetooth specification contains the Bluetooth Radio Specification as well as the Baseband, Link Manager, L2CAP, Service Discovery, RFCOMM and other specifications.



Bluetooth

- The Bluetooth specification allows for three different types of radio powers:
  - Class 1 = 100mW
  - Class2 = 2.5mW
  - Class 3 = 1mW
- These power classes allow Bluetooth devices to connect at different ranges
- High power radius have longer ranges. The maximum range for a Class 1, 100mW is about 100 meters. There is also a minimum range for a Bluetooth connection. The minimum range is around 10cm.

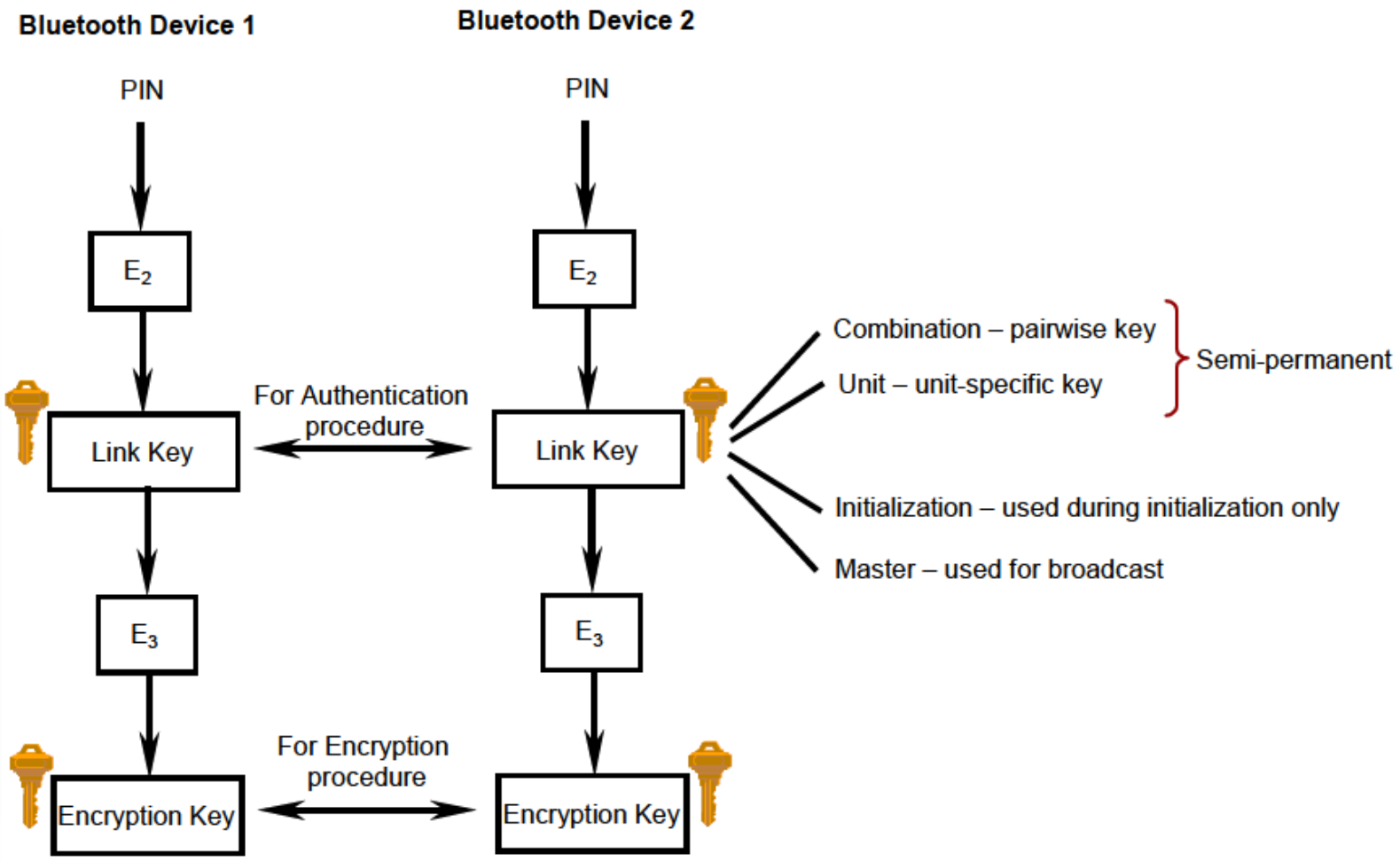
Bluetooth

- **Cable Replacement**
  - Replace the cables for peripheral devices
- **Ease of file sharing**
  - Panel discussion, conference, etc.
- **Wireless synchronization**
  - Synchronize personal information contained in the address books and date books between different devices such as PDAs, cell phones, etc.
- **Bridging of networks**
  - Cell phone connects to the network through dial-up connection while connecting to a laptop with Bluetooth.

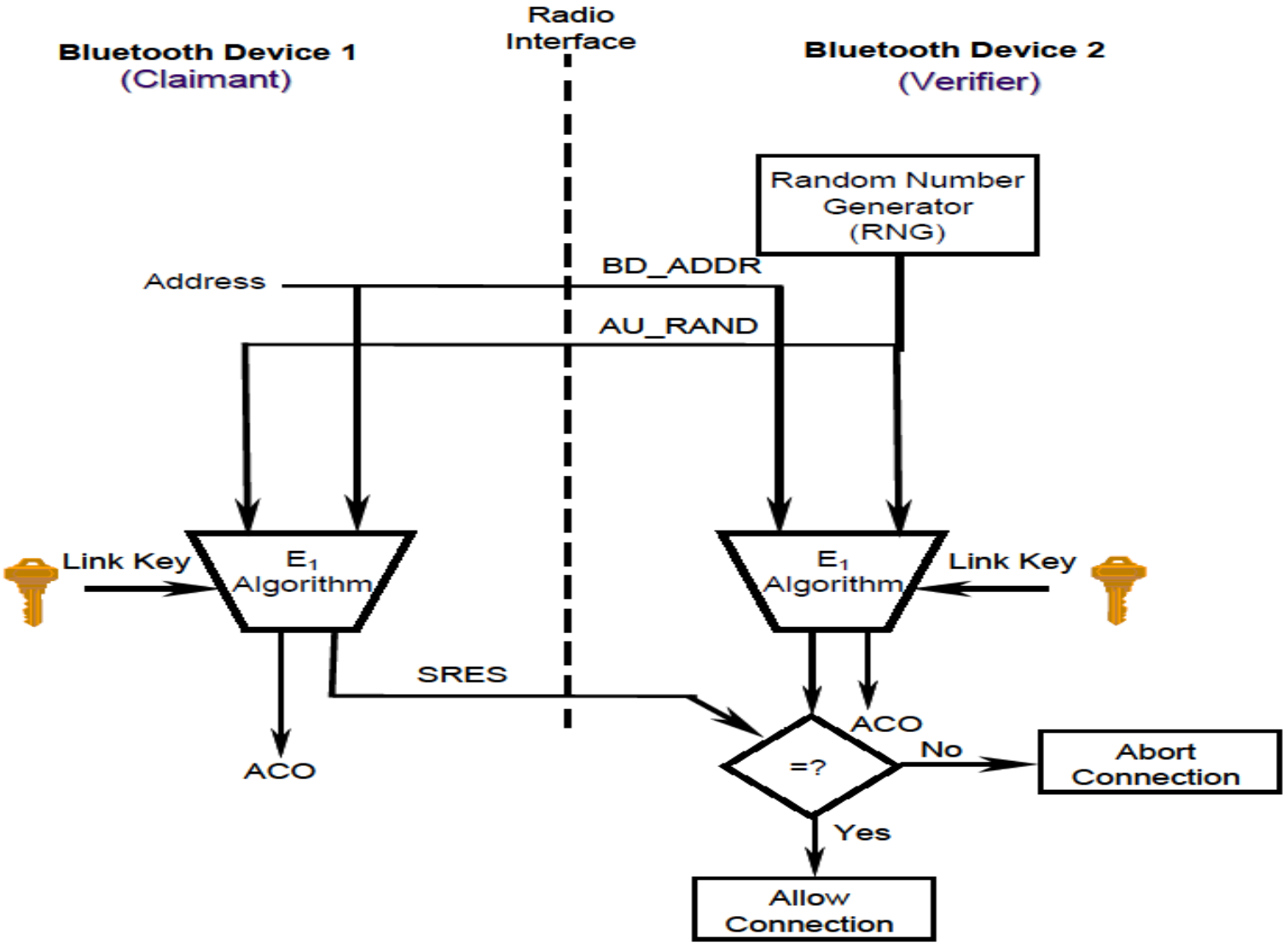
Bluetooth Security Modes

- **Security Mode 1** is non-secure
- **Security Mode 2** controls access to certain services and uses a security manager. But this is only initiated after a link is established. Mode 2 has three levels:
- Level 1: Open to all devices, the default level.
- Level 2: Authentication only.
- Level 3: Requires Authentication and Authorization. PIN number must be entered.
- **Security Mode 3** initiates security procedures before any link is established. It supports authentication and encryption. The NIST considers this the most secure.
- **Security mode 4** requires authenticated links, but like mode 2 only initiates the authentication and encryption after a link is established

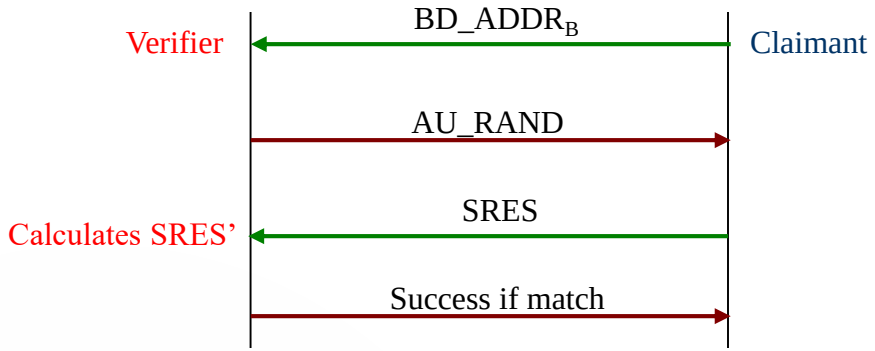
Link Key Generation



Authentication



Authentication Summary

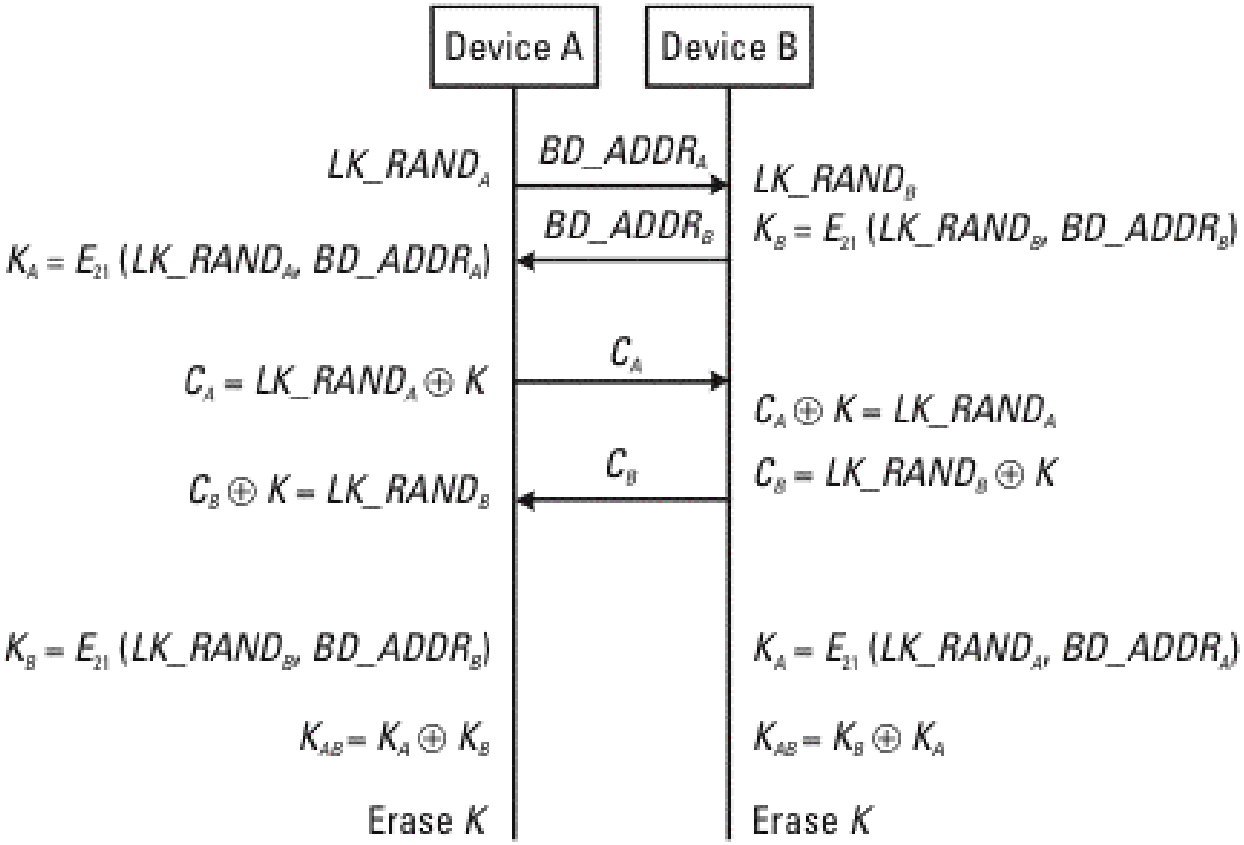


Authentication Process

Parameter	Length	Secrecy parameter
Device Address	48 Bits	Public
Random Challenge	128 Bits	Public
Authentication (SRES) Response	32 Bits	Public
Link Key	128 Bits	Secret

Confidentiality

Confidentiality security service protects the eavesdropping attack on air-interface.



Bluetooth Encryption Process

- ***Encryption Mode 1:*** No encryption is needed.
- ***Encryption Mode 2:*** Encrypted using link key keys.
- ***Encryption Mode 3:*** All traffic is encrypted.

Trust levels, service levels and authentication

- ***Service level 1:*** Requires authentication and authorization.
- ***Service level 2:*** Requires only authentication.
- ***Service level 3:*** Open to all bluetooth devices.

Problems with the standard Bluetooth Security

Security Issue	Remarks
Strength of the Random Number Generator (RNG) is unknown.	RNG may produce periodic numbers that reduces the strength of authentication mechanism.
Short PINs are allowed.	Such weak PINs are used to generate link and encryption keys that are easily predictable.
Encryption key length is negotiable.	More robust initialization key generation procedure should be developed.
No user authentication exists.	As only device authentication is provided, application security and user authentication can be employed.
Stream cipher is weak and key length is negotiable.	Robust encryption procedure and minimum key length should be decided and passed as an agreement.

Bluetooth

Security Issue	Remarks
Privacy can be compromised if the BD_ADDR is captured and associated with a particular user.	Once the BD_ADDR is associated with a particular user, that user's activity can be logged. So, loss of privacy can be compromised.
Device authentication is simple shared key challenge response.	One-way authentication may be subjected to man-in-middle attacks. Mutual authentication is a good idea to provide verification.

Other Wireless

- ANT+ is a wireless protocol often used with sensor data such as in bio sensors or exercise applications.
- Near Field Communication (NFC) works if the two devices are within 4 cm (1.6 inches) of each other. Operates on globally available unlicensed radio frequency ISM band of 13.56 MHz on ISO/IEC 18000-3 air interface at rates ranging from 106 to 424 kbit/s. NFC is standardized in ECMA-340 and ISO/IEC 18092.

Bluetooth attacks

Blue snarfing is a class of attacks wherein the attacker attempts to get data from the phone.

Bluejacking is sending unsolicited data to a phone, via Bluetooth. This is sometimes used to send spam instant messages.

Blue smacking is a Denial of Service attack where in the target is flooded with packets.

Blue bugging remotely accesses phone features. This may seem very similar to Blue snarfing, but the goal with Blue bugging is not to get data, but to activate certain phone features.

Blue sniffing is the same thing as war driving. The attacker is trying to find available Bluetooth devices to attack.

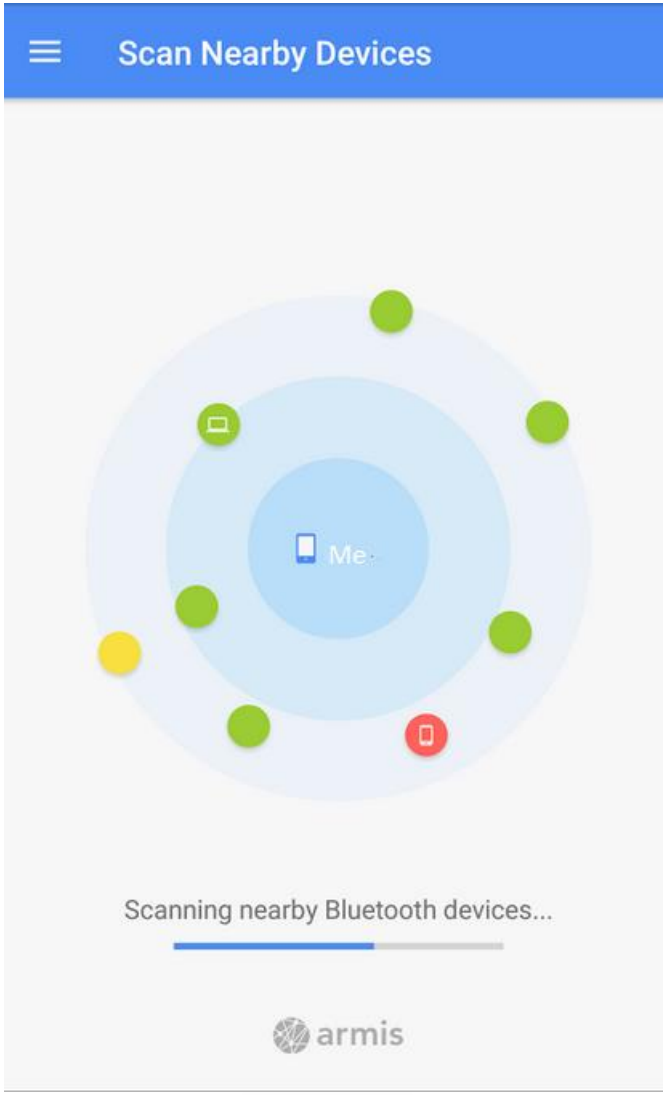
Blue printing gets its name from foot printing. In the case of Blue printing, the attacker is trying to get information about the target phone.

BH Blue Jack

- This tool is available as open source (i.e. free) and is written in Python. It allows you to attempt Bluejacking with the click of a button.
- http://www.bluejackingtools.com/symbian/bh-bluejack-bluejacking-software/

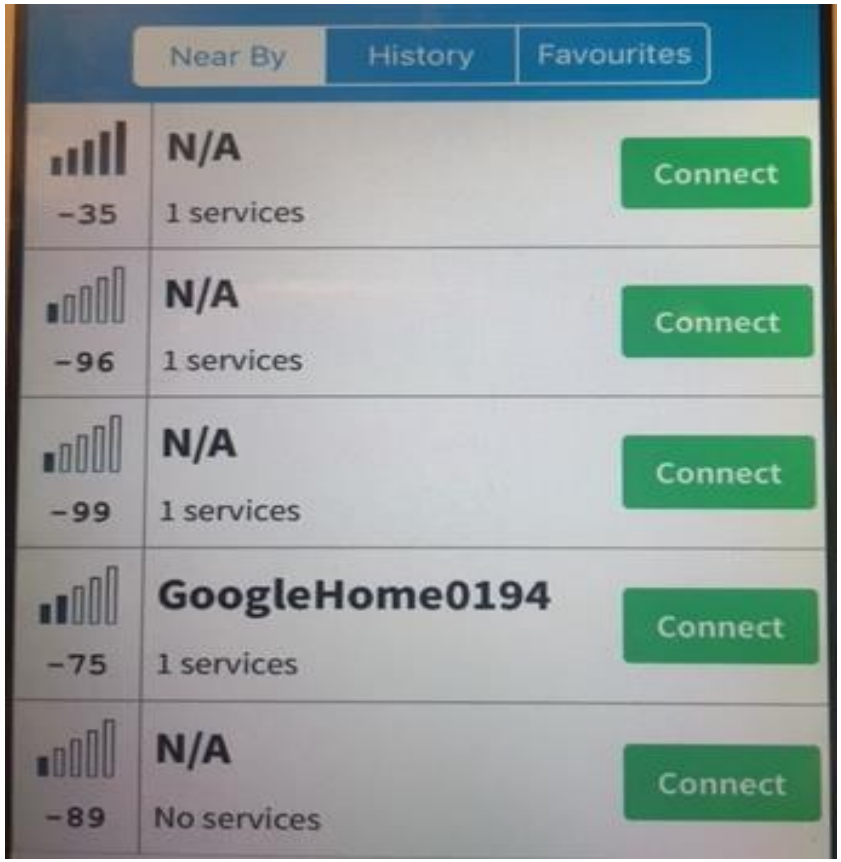
Blueborne

This is a vulnerability scanner for Bluetooth. It is available in the Google play store for Android phones, and you can see it here: https://play.google.com/store/apps/details?id=com.armis.blueborne_detector&hl=en. The vendor also has a white paper on Bluetooth vulnerabilities, you can view it here: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf



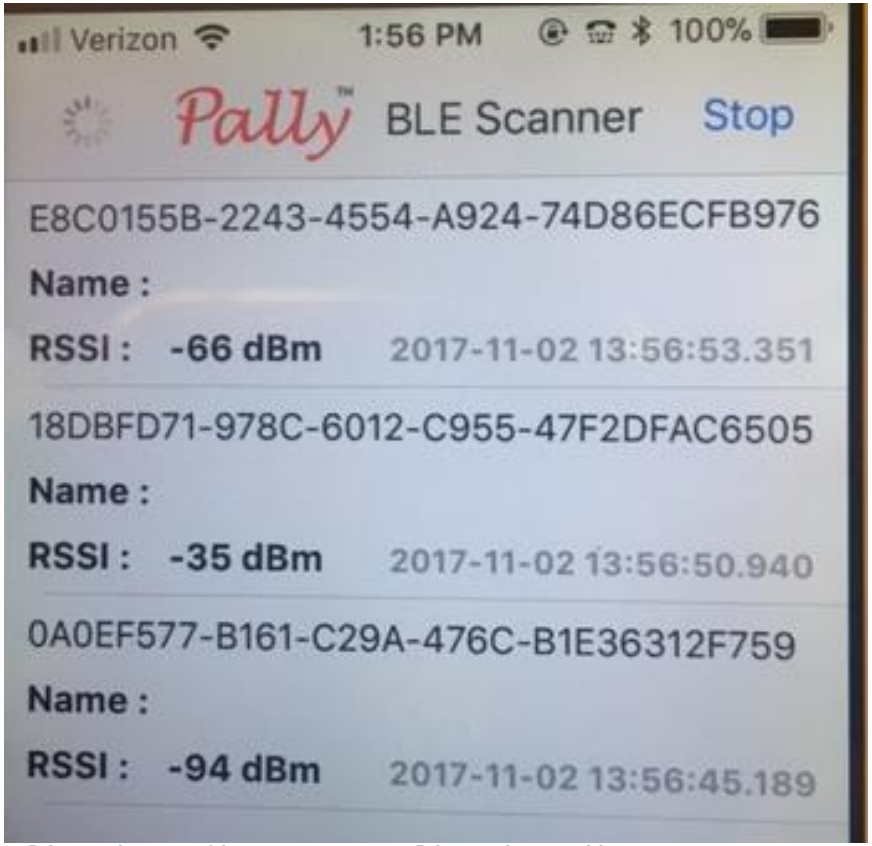
BLE Scanner

This tool is for the iPhone and is a free download. The first thing it will do is show you nearby Bluetooth



Pally

Pally is another Bluetooth scanner for the iPhone. It has an easy to user interface and will provide you basic information about nearby Bluetooth devices



Other tools

- PhoneSnoop
- Bluescanner
- BH BlueJack
- Bluesnarfer
- btCrawler
- Bluediving
- Bloover II
- btscanner
- CIHwBT
- BT Audit
- Blue Alert
- Blue Sniff

Bluetooth

- Problems with E0
- PIN
- Problems with E1
- Location privacy
- Denial of service attacks

Bluetooth

- Given all cryptographic primitives (E0, E1, E21, E22) used in Bluetooth Pairing/Bonding and authentication process the Bluetooth PIN can be cracked.
- Output (KC) = combination of 4 LFSRs (Linear Feedback Shift Register)
- Key (KC) = 128 bits
- Best attack: guess some registers

Attack Surface

- “An attack vector generally refers to the means by which an attacker makes his move.”
- “An attack surface is generally understood as a target's open flanks— that is to say, the characteristics of a target that makes it vulnerable to attack”

- Drake, Joshua J.; Lanier, Zach; Mulliner, Collin; Oliva Fora, Pau; Ridley, Stephen A.; Wicherski, Georg. Android Hacker's Handbook

Vulnerability

- CVSS – Common Vulnerability Scoring System
- https://www.first.org/cvss/
- The CVSS assessment measures three areas of concern:
- Base Metrics for qualities intrinsic to a vulnerability
- Temporal Metrics for characteristics that evolve over the lifetime of vulnerability
- Environmental Metrics for vulnerabilities that depend on a particular implementation or environment

Vulnerability

- National Vulnerability Database
- https://nvd.nist.gov/
- The National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program (ISAP).

Vulnerability

- Common Vulnerabilities and Exposures
- https://cve.mitre.org/
- CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
- CVE Entries are used in numerous cybersecurity products and services from around the world,
- including the U.S. National Vulnerability Database (NVD).

Use your phone as a hacking platform

- Some techniques may require that the phone must be rooted
- Framaroot latest apk - http://www.apkmods.net/2015/05/framaroot-apk-latest-v193-for-andriod.html
- Kingroot latest apk - https://docs.google.com/uc?export=download&id=0B6rbGz1rR1IgYVVZQkhqUjJmTWs

Fing Wifi Network Analyzer Toolkit for Android

- Fing android app is scan wifi network ,and you see all connected devices in your wifi network.
- Fing give detail information about every connected devices like mac,vendor name,manufacturer,ip address and more.
- http://www.prophethacker.com/2014/06/fing-wifi-network-analyzer-toolkit-for-android.html

USB Cleaver

- To use the application, hacker must install an application called USB Cleaver on his Android device. Once executed, the app downloads a ZIP file from a remote server and then unzips the downloaded file to the following location: */mnt/sdcard/usbcleaver/system* folder.
- Tools is design to steal information like Browser passwords (Firefox, Chrome and IE), PC's Wi-Fi password, The PC's network information etc.
- When the device is then plugged into a PC, */mnt/sdcard* is mounted and, if *autorun* is enabled, go.bat and the payload are executed. The app allows the user to select what type of information should be harvested. The utilities save their results in */mnt/sdcard/usbcleaver/logs* which the app user can view later by clicking "*Log files*" in the app.

WPS Connect

- Attempt to hack WPS if it is being used http://www.prophethacker.com/2015/06/hack-wifi-network-android.html

inSSIDer

- Find wi-fi even if the SSID is not broadcast
- For Android
  https://inssider.en.uptodown.com/android

Ghost Phone

- https://play.google.com/store/apps/details?id=com.rungetel.ghostphone&hl=en_US
- Lets you change IMEI of the phone

Change My Mac Lite

- Change your phone mac address
- https://play.google.com/store/apps/details?id=net.xnano.android.changemymac.lite&hl=en_US

Network Spoofer

- https://www.digitalsquid.co.uk/netspoof/
- Flip pictures upside down
- Flip text upside down
- Make websites experience gravity
- Redirect websites to other pages
- Delete random words from websites
- Replace words on websites with others
- Change all pictures to Trollface
- Wobble all pictures / graphics around a bit

Other tools

- Wi Fi Kill Knock others off the Wi Fi
  https://wifikillapk.com/download/
- CSPloit a general penetration testing kit
  http://www.csploit.org/downloads/
- Wifi Wps Wpa Tester tries to crack Wi-Fi
  https://play.google.com/store/apps/details?id=com.tester.wpswpatester&hl=en_US

Hackode

- https://apkpure.com/hackode/com.techfond.hackode
  - This is a penetration testing kit for Android.
- Faceniff
- http://faceniff.ponury.net/

- USBCleaver
- https://forum.xda-developers.com/showthread.php?t=1656497
- This app lets you steal data from a PC/Laptop via USB connection