BAKI ALİ NEFT MƏKTƏBİ
BAKU HIGHER OIL SCHOOL

Mobile development and security

Session 17

Karim Karimov

Lecturer

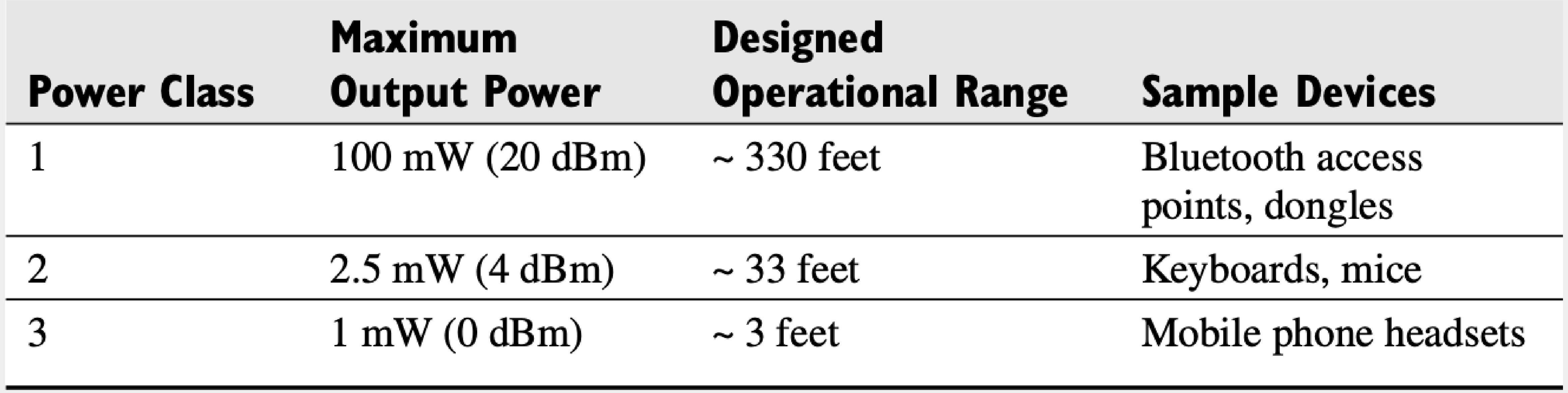
Bluetooth

Bluetooth was originally conceived as an internal project at Ericsson Mobile Communications to create a wireless keyboard system. The technology proved to be useful for other objectives, and additional work was performed within Ericsson to apply the wireless connectivity to more generic purposes. To further the development and acceptance of the technology, the Bluetooth Special Interest Group (SIG) was formed in 1998 to help shepherd the emerging standard and promote the spread of Bluetooth to other practical applications (Bluetooth Security). Since 1998, the Bluetooth SIG has administered and published the Bluetooth specifications and managed, marketed, and evangelized the technology.

Radio Operation and Frequency

Bluetooth radios operate in the unlicensed ISM band at 2.4GHz (also used by 802.11 networking equipment, microwave ovens, and many cordless phones). Bluetooth radios implement frequency-hopping spread spectrum for data transmission. Transmission rates are up to 1Mbps for most devices, although devices running Enhanced Data Rate (available with Bluetooth versions 2.0 and 2.1) can have rates up to 2Mbps or 3Mbps.

The Bluetooth specification defines three transmitter power classes. The class of radio used for a Bluetooth device is determined primarily based on usage and proximity requirements and power availability (that is, AC powered versus battery powered).



Power Class	Maximum Output Power	Designed Operational Range	Sample Devices
1	100 mW (20 dBm)	~ 330 feet	Bluetooth access points, dongles
2	2.5 mW (4 dBm)	~ 33 feet	Keyboards, mice
3	1 mW (0 dBm)	~ 3 feet	Mobile phone headsets

Discoverability Modes

Discoverability refers to whether or not the configured device will respond to discovery inquiries from other Bluetooth devices. The defined discoverability modes include:

- **Non-discoverable** Devices in this mode do not respond to inquiry scans from other devices. Note that this does not mean that the devices cannot be connected to (this characteristic is specified and controlled by the Bluetooth connectability modes).
- **Limited discoverable mode** This mode is used by devices that need to be discoverable for a limited amount of time.
- **General discoverable mode** This mode is used by devices that are continuously discoverable by other devices. Devices in either limited or general discoverable mode periodically listen to an inquiry physical channel and respond to inquiry scans with a set of connection configuration information that allows the scanning device to begin to initiate a connection with the responding device.

Connectability Modes

Connectability refers to whether or not the configured device will respond to paging from other devices (that is, requests to initiate a Bluetooth connect). The defined connectability modes include:

- **Non-connectable mode** Devices in this mode never enter the page scan state, meaning they will never receive/acknowledge/respond to a page request and are not able to establish connections based on inbound page requests.
- **Connectable mode** Devices in this mode will periodically enter the page scan state. This means that the device listens for pages on the page scan physical channel and will respond to pages (connection requests).

Pairability/Bondability Modes

Pairability refers to whether a device is capable of bonding/pairing with another Bluetooth device. The defined bondability modes include:

- **Non-bondable mode** Devices in this mode do not respond to bonding requests and will not pair with other devices.
- **Bondable mode** Devices in bondable mode will allow pairing with another Bluetooth device. Note that devices in bondable mode may require additional security prior to pairing (that is, PIN entry/authentication).

Bluetooth Security Features

Bluetooth is designed to provide cable-free operation and interaction among a variety of devices, many of which tend to be consumer electronic devices. Because of the variety of devices in use and the situations for which Bluetooth is intended, no assumptions can be made about either the Bluetooth device or the technical sophistication of the device’s user. Bluetooth must be usable by novice consumers and on devices with limited or no visual display or input capabilities (headsets, keyboards, and so on). So, a key factor that complicates Bluetooth security is that many usage scenarios involve nontechnical users as well as devices that are incapable of the security mechanisms a developer may wish to use.

It is important that these issues remain at the top of mind as mobile application developers plan the design of their applications, as well as whether and how these applications will leverage or rely on Bluetooth security.

Pairing

Pairing, the process whereby two Bluetooth devices establish a link and agree to communicate, is critical to the overall security architecture of Bluetooth and is tightly integrated with other Bluetooth security features. During the pairing process, the communicating devices agree on and generate keys that are used to identify and reference relationships with other devices. In addition to being used for these identification purposes, these keys are also used to generate additional keys used for both device authentication and communication encryption.

Device Pairing Prior to Bluetooth v2.1 + EDR

In versions prior to Bluetooth v2.1 + EDR (released in July 2007), pairing between devices is accomplished through the entry of a PIN or passkey with a maximum length of 128 bits. There are two types of such passkeys: **variable passkeys**, which can be chosen at the time of pairing via some input mechanism, and **fixed passkeys**, which are predetermined. The type of passkey used is typically determined by a device's input and display capabilities (for example, a Bluetooth-enabled phone with keyboard input and visual display may use a variable passkey, whereas a Bluetooth-enabled mouse may use a fixed passkey because it has neither input nor display capabilities to enter or verify a passkey).

Secure Simple Pairing with Bluetooth v2.1 + EDR

In Bluetooth v2.1 + EDR, a new method of pairing called Secure Simple Pairing was introduced. The older method of pairing is supported when connecting to legacy devices, but the use of Secure Simple Pairing is mandated for communications between Bluetooth v2.1 + EDR devices.

From a user's perspective, Secure Simple Pairing is meant to provide additional flexibility and ease of use when pairing compatible devices that have far-ranging display and input capabilities. However, from a security perspective, Secure Simple Pairing also improves security through the introduction of **Elliptic Curve Diffie-Hellman** (**ECDH**) for key exchange and link key generation.

Rather than relying on simple PIN/passkey entry and verification, Secure Simple Pairing offers four different means for pairing compatible devices (known as association models).

Secure Simple Pairing with Bluetooth v2.1 + EDR

1. **Numeric Comparison** This association model is designed for situations where both communicating devices can display a six-digit number and have inputs that allow the user to enter “yes” or “no.” A six-digit number from 000000 to 999999 is shown on both displays, and the user is prompted to respond whether the numbers are the same on both devices. If “yes” is entered on both devices, then the devices are paired successfully. Note that a primary difference between Numeric Comparison and the PIN model used in legacy pairing is the displayed number. In Numeric Comparison, this value is not used as an input to further key generation, so an attacker who can observe the displayed number cannot use it to calculate other keys. With the legacy PIN model, the PIN entered does factor into the generation of encryption keys, which makes PIN disclosure a real risk to the security of the communications.

Secure Simple Pairing with Bluetooth v2.1 + EDR

2. **Just Works** This association model is intended for scenarios involving at least one device without the ability to display a six-digit number or to enter numbers. This mode uses the same key agreement protocol as Numeric Comparison (with protections against passive eavesdropping), but the actual method whereby the user accepts the Bluetooth connection is determined by the product manufacturer. This association model does not provide protection against man-in-the-middle attacks.

Secure Simple Pairing with Bluetooth v2.1 + EDR

3. **Out of Band** This association model is intended for scenarios involving an out-of-band (OOB) mechanism (that is, non-Bluetooth) that is used to both discover the Bluetooth devices and exchange information during the pairing process. The actual OOB mechanism will vary, but a commonly specified use case involving a **Near Field Communication** (**NFC**) OOB mechanism is device “tapping.” This use case involves physically touching two devices together.

Subsequent to the devices being tapped together, the user is asked to confirm whether the pairing request initiated by the tapping should be accepted. To provide security for the pairing process, the OOB mechanism used should provide privacy protections, including resistance to man-in-the-middle attacks.

Secure Simple Pairing with Bluetooth v2.1 + EDR

4. **Passkey Entry** This association model is intended primarily for situations involving one device with input capabilities but no display capabilities while the other device has display capabilities. The device with a display presents a six-digit number from 000000 to 999999 on the display. The user then enters this number on the device with the input capability. If the values match, then the devices are paired successfully.

Traditional Security Services

The Bluetooth specifications include a limited set of these basic security services, and as such, the level of security that can be implemented with native Bluetooth features is limited. The following security services are provided by the Bluetooth specification:

- **Authentication** The ability to identify devices before and during connection and communication is provided by Bluetooth.
- **Authorization** The ability to provide selected access to resources based on permissions is provided by Bluetooth.
- **Confidentiality** The ability to protect communications during transmission over the network is provided by Bluetooth.

Noticeably absent are integrity protections and nonrepudiation services. In addition, native Bluetooth security services are provided at the device-to-device level; for instance, Bluetooth's authentication service only authenticates a Bluetooth device. There is no provision for user-level authentication.

Authentication

Bluetooth authentication is the process whereby one device verifies the identity of another device. Bluetooth authentication is a one-way process, meaning that during any given authentication procedure, only one device’s identity is verified.

Bluetooth authentication involves the **claimant** device, which is the device that will have its identify verified by the authentication process, and the verifier device, which is the device that will verify the claimant’s identity. To perform this verification, a traditional challenge-response mechanism is used.

The Bluetooth authentication mechanism has a simple protection to prevent repeated attacks in a limited timeframe. When an authentication attempt fails, the verifier will delay its next attempt to authenticate the claimant. This delay interval will be increased exponentially for each subsequent failed attempt.

Authorization

Authorization in Bluetooth allows for decision making about resource access and connection configuration (that is, authentication and encryption requirements) to be made based on the permissions granted a given Bluetooth device or service. Two of the primary means of implementing authorization in Bluetooth are device trust levels and service security levels.

Device Trust Levels Bluetooth devices can have one of two trust levels in relation to other Bluetooth devices: trusted or untrusted (refer to the "Wireless Security" page at the Bluetooth website).

- **Trusted devices** have previously been paired with the device, and will have full access to services on the Bluetooth device.
- **Untrusted devices** have not previously been paired with the device (or the relationship has been otherwise removed), and will have restricted access to services.

Authorization

Service Security Levels Bluetooth services (applications that use Bluetooth) have one of three security levels:

- **Service Level 1** These services require device authentication and authorization. Trusted devices will be granted automatic access to these services. Manual authentication and authorization will be required before untrusted devices are granted access to these services.
- **Service Level 2** These services require authentication, but do not require authorization.
- **Service Level 3** These services have no security and are open to all devices.

Although Bluetooth’s notions of device trust and service security levels are quite simple, the architecture of Bluetooth does provide for the implementation of more complex security and authorization policies.

Confidentiality

Confidentiality is important for private communications over wireless links because the nature of wireless networking leaves the communication between nodes subject to eavesdropping by unauthorized parties. Confidentiality of network communications in Bluetooth is provided through the use of encryption, with the use of encryption being optional and determined by the selection of one of three encryption modes during communication.

- **Encryption Mode 1** No encryption. All traffic is unencrypted when Encryption Mode 1 is used.
- **Encryption Mode 2** Traffic between individual endpoints (non-broadcast) is encrypted with individual link keys. Broadcast traffic is unencrypted.
- **Encryption Mode 3** Both broadcast and point-to-point traffic is encrypted with the same encryption key (the master link key). In this mode, all traffic is readable by all nodes in the piconet (and remains encrypted to outside observers). Note that the notion of privacy in Encryption Mode 3 is predicated on the idea that all nodes in the piconet are trusted because all nodes will have access to the encrypted data.

Security “Non-Features”

In addition to reviewing the actual security features provided by Bluetooth, it is useful to acknowledge and refute two characteristics of Bluetooth communications that may be claimed as security features but do not provide any real protection:

- **Frequency hopping** The frequency-hopping scheme that Bluetooth uses does not provide any protection against eavesdropping. There is no secret used to create the sequence of channels, and only 79 channels are used. Thus, using a series of receivers to monitor all channels would make an offline attack possible.
- **Device proximity** The limited range of Bluetooth radios (up to approximately 330 feet with Class 1 radios) cannot be reliably used as a security feature. The supposed protection provided by limited signal strength can and has been defeated by attackers’ high gain antennas.

Threats to Bluetooth Devices and Networks

- **Location tracking** Because Bluetooth devices by their nature emit radio signals and device addresses must be both unique and known to communicating parties, Bluetooth devices are subject to location-tracking threats.
- **Key management issues** Like many technologies that use cryptography for features such as authentication and encryption, Bluetooth devices are subject to threats related to key management, including key disclosure or tampering.
- **Bluejacking** Bluejacking involves the sending of unsolicited messages to a victim’s Bluetooth device. This can be leveraged as a social-engineering attack that is enabled by susceptible Bluetooth devices.

Threats to Bluetooth Devices and Networks

- **Implementation issues** Implementation flaws become threats when a product manufacturer incorrectly implements the Bluetooth specification in its device, making the device or communications subject to security issues that would not exist if the specification was implemented correctly. Implementation flaws have been at the root of many well-known Bluetooth security issues, including:
    - **Bluesnarfing** This attack allows access to a victim Bluetooth device because of a flaw in device firmware. Arbitrary data can be accessed through this attack, including the International Mobile Equipment Identity (IMEI).
    - **Bluebugging** This attack allows an attacker to access data, place calls, and eavesdrop on calls, among other activities. This attack is made possible by a firmware flaw on some mobile phones.
    - **Car whispering** This attack allows an attacker to send or receive audio via a Bluetooth-enabled hands-free automobile kit. This attack is made possible due to an implementation flaw on these kits.

Bluetooth Vulnerabilities

Bluetooth Versions Prior to v1.2

- The unit key is reusable and becomes public when used. The unit key is a type of link key generated during device pairing, and has been deprecated since Bluetooth v1.2. This issue allows arbitrary eavesdropping by devices that have access to the unit key.

Bluetooth Versions Prior to v2.1

- Short PINs are permitted. Because PINs are used to generate encryption keys and users may tend to select short PINs, this issue can lower the security assurances provided by Bluetooth’s encryption mechanisms.
- The encryption keystream repeats. In Bluetooth versions prior to v2.1, the keystream repeats after 23.3 hours of use. Therefore, a keystream is generated identical to that used earlier in the communication.

Bluetooth Vulnerabilities

All Versions

- **Unknown random number generator (RNG) strength for challenge-response** The strength of the RNG used to create challenge-response values for Bluetooth authentication is unknown. Weaknesses in this RNG could compromise the effectiveness of Bluetooth authentication and overall security.
- **Negotiable encryption key length** The Bluetooth specification allows the negotiation of the encryption key down to a size as small as one byte.
- **Shared master key** The encryption key used to key encrypted broadcast communications in a Bluetooth piconet is shared among all piconet members.
- **Weak E0 stream cipher** A theoretical known-plaintext attack has been discovered that may allow recovery of an encryption key much faster than a brute-force attack.
- **Limited security services** As mentioned previously, Bluetooth offers a limited set of security services, with services such as integrity protection and nonrepudiation excluded.

Recommendations

Do not rely on Bluetooth’s native security mechanisms for sensitive applications. Because Bluetooth provides only device-level security services (versus user level), Bluetooth’s security controls cannot be relied upon to limit access to sensitive data and applications to authorized users.

- Use complex PINs for Bluetooth devices.
- In sensitive and high-security environments, configure Bluetooth devices to limit the power used by the Bluetooth radio.
- Avoid using the “Just Works” association model for v2.1 + EDR devices.
- Limit the services and profiles available on Bluetooth devices to only those required.
- Configure Bluetooth devices as non-discoverable except during pairing. Avoid use of Security Mode 1.
- Enable mutual authentication for all Bluetooth communications. Configure the maximum allowable size for encryption keys.

Geolocation on mobile

Mobile devices store and share device geolocation data by design. This data is essential to device communications and provides features—such as mapping applications—that users consider indispensable. Mobile devices determine location through any combination of Global Positioning System (GPS) and wireless signals (e.g., cellular, wireless (Wi-Fi®), or Bluetooth® (BT)). Location data can be extremely valuable and must be protected. It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations. Mitigations reduce, but do not eliminate, location tracking risks in mobile devices. Most users rely on features disabled by such mitigations, making such safeguards impractical. Users should be aware of these risks and take action based on their specific situation and risk tolerance.

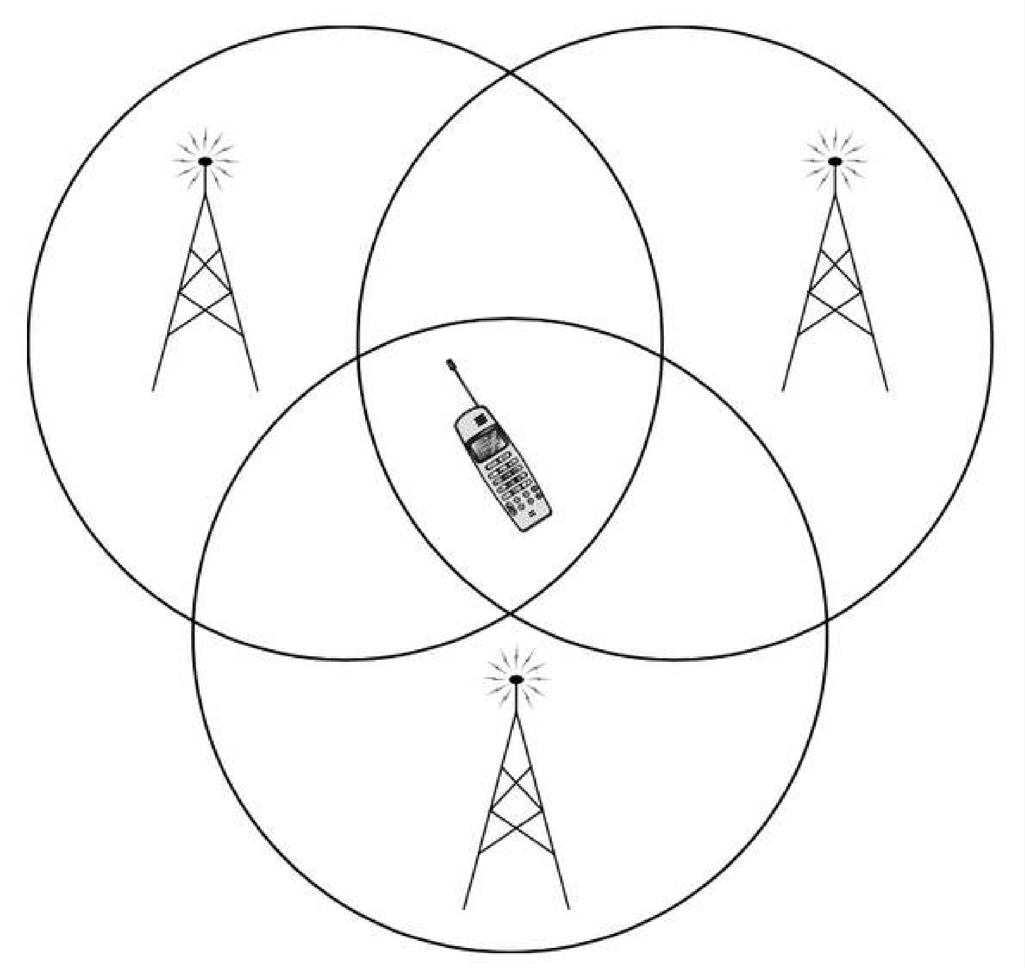
Geolocation Methods

Geolocation on mobile devices has grown from being used solely for emergency and law enforcement purposes to being an integral component of consumer mobile applications. Once only performed by triangulation of cell towers, modern mobile OSes have expanded to support retrieval of positional data via wireless survey or GPS systems, giving an enhanced degree of precision and faster update times. Different methods have their own strengths and weaknesses, along with variations in accuracy.

Tower Triangulation

Accuracy: 50m–1,000m

Tower triangulation is the oldest widely used method of geolocation via cell phone. This method uses the relative power levels of radio signals between a cell phone and a cell tower of a known location—this of course requires at least two cell towers to be within range of the user. This service is used for the E911 system in the United States, transmitting location data when emergency calls are made. With user permission, however, the phone can be instructed to transmit tower triangulation data to phone applications. Because this requires that the user be near to multiple cells, and because signal strength can be affected by many factors, tower triangulation is a fairly inexact method of positioning.



GPS

Accuracy: 5m–15m

Using satellite signals instead of cell phone or wireless infrastructure, GPS service is often available at times when other methods are not. However, satellite acquisition is generally impaired when the user is indoors, making the use of GPS alone inadequate for some mobile applications. Additionally, initial GPS location information can take several minutes to acquire.

An advantage of GPS is that it can provide continuous tracking updates, useful for real-time applications, instead of just one-time lookups.

Assisted GPS works by providing an initial location obtained via another means (either tower triangulation or 802.11) to the GPS receiver, to reduce satellite acquisition time and correct for signal noise. This makes GPS somewhat more viable for indoor use; however, acquiring positional data this way still takes upwards of 10 seconds, still making it a relatively slow method.

802.11

Accuracy: 10m–200m (but potentially erroneous)
The iPhone was the first smartphone to add this additional method for geolocation, using an API made available by Skyhook Wireless. This location method works by doing a survey of any nearby 802.11 (Wi-Fi) wireless access points and then submitting data about them (presumably MAC address and SSID) to a web service, which returns coordinates from what is essentially a very large "wardriving" database. This allows for devices without GPS to provide potentially highly accurate location data.

This approach has the advantage of being both faster and much more accurate than cell tower triangulation, but has a couple of drawbacks. Because location data relies on specific wireless APs, if those APs move, location data can be drastically wrong.

Geolocation Implementation

Android

As with most services on Android, permission to use the geolocation features is requested via the program manifest and is granted by the user either at install time (up to Android 6), or during runtime. Either coarse or fine precision can be requested, using the **ACCESS_COARSE_LOCATION (for cell triangulation or Wi-Fi)** or **ACCESS_FINE_LOCATION (GPS)** permission.

iPhone

Geolocation on the iPhone requires user approval every time an application that uses geolocation APIs is launched.There are several constants when requesting locational data:

```
    const CLLocationAccuracy kCLLocationAccuracyBest;
    const CLLocationAccuracy kCLLocationAccuracyNearestTenMeters;
    const CLLocationAccuracy kCLLocationAccuracyHundredMeters;
    const CLLocationAccuracy kCLLocationAccuracyThreeKilometers;
```

Mobile exposes location data

Using a mobile device—even powering it on—exposes location data. Mobile devices inherently trust cellular networks and providers, and the cellular provider receives real-time location information for a mobile device every time it connects to the network. This means a provider can track users across a wide area.

Location data from a mobile device can be obtained even without provider cooperation. These devices transmit identifying information when connecting to cellular networks. Commercially available **rogue base stations** allow anyone in the local area to inexpensively and easily obtain real-time location data and track targets. This equipment is difficult to distinguish from legitimate equipment, and devices will automatically try to connect to it, if it is the strongest signal present.

Additionally, location data is **stored on the mobile device**. Past location information can be used to forecast future locations Other examples of risk exist: websites use browser fingerprinting to harvest location information, and Wi- Fi access points and Bluetooth sensors can reveal location information.

Location services ≠ GPS

A mobile device provides geolocation data as a service to apps. This is known as location services, and users can disable them in the settings of a device. Perhaps the most important thing to remember is that disabling location services on a mobile device does not turn off GPS, and does not significantly reduce the risk of location exposure. Disabling location services only limits access to GPS and location data by apps. It does not prevent the operating system from using location data or communicating that data to the network. Also important to remember is that GPS is not the same as location services. Even if GPS and cellular data are unavailable, a mobile device calculates location using Wi-Fi and/or BT. Apps and websites can also use other sensor data (that does not require user permission) and web browser information to obtain or infer location information.

Other equipments determine location

Even if cellular service is turned off on a mobile device, Wi-Fi and BT can be used to determine a user’s location. Inconspicuous equipment (e.g., wireless sniffers) can determine signal strength and calculate location, even when the user is not actively using the wireless services. Even if all wireless radios are disabled, numerous sensors on the device provide sufficient data to calculate location. Disabling BT completely may not be possible on some devices, even when a setting to disable BT exists. When communication is restored, saved information may be transmitted. If a mobile device has been compromised, the user may no longer be able to trust the setting indicators. Detecting compromised mobile devices can be difficult or impossible; such devices may store or transmit location data even when location settings or all wireless capabilities have been disabled.

IoT devices

Anything that sends and receives wireless signals has location risks similar to mobile devices. This includes, but is not limited to, fitness trackers, smart watches, smart medical devices, Internet of Things (IoT) devices, and built-in vehicle communications. Personal and household smart devices (e.g., light bulbs, cookware, thermostats, home security, etc.) often contain wireless capabilities of which the user is unaware. Such IoT devices can be difficult to secure, most have no way to turn off wireless features, and little, if any, security built in. These security and privacy issues could result in these devices collecting and exposing sensitive location information about all devices that have come into range of the IoT devices. Geolocation information contained in data automatically synced to cloud accounts could also present a risk of location data exposure if the accounts or the servers where the accounts are located are compromised.

Apps and social media

Apps, even when installed using the approved app store, may collect, aggregate, and transmit information that exposes a user’s location. Many apps request permission for location and other resources that are not needed for the function of the app. Users with location concerns should be extremely careful about sharing information on social media. If errors occur in the privacy settings on social media sites, information may be exposed to a wider audience than intended. Pictures posted on social media may have location data stored in **hidden metadata**. Even without explicit location data, pictures may reveal location information through picture content.

Risks of Geolocation Services

Although mobile geolocation services have resulted in some useful and convenient mobile applications, these services expand the potential risks to both the end user and the remote service providers making use of this data. Any tracking technology has the capacity to make software more personalized, but this very personalization is what makes it attractive to law enforcement and civil trial lawyers, as well as other malicious parties.

Risks to the End User (EU)

Positional data stored on remote servers, when it can be tied to an individual, introduces a new avenue for data theft. Not only can a compromise of a sensitive service reveal personal and credit card data, it can also reveal information about users' historical whereabouts, potentially over an extended timeframe. This is not only a breach of user privacy, but potentially provides information that can be used against a user in court.
End users of geolocation technologies should take the following into account:

- Does the application/site have a privacy policy for positional information?
- Is data retained or discarded/overwritten?
- If data is retained, will records be handed over to law enforcement upon request, or is a court order required?
- Does the provider share location data with third parties or store data with them?
- Are other users of the service privy to your location data?
- Are you able to easily block users?

Risks to Service Providers (SP)

By maintaining extended positional records on users, service providers expose themselves to the risk of negative publicity from a data breach, legal or congressional subpoenas, and potential assistance to criminal acts by allowing third parties to track individual users. Often, this data isn't really necessary to provide the required functionality. In some places, you as a provider will have a legal obligation to follow privacy guidelines. For example, in the UK, the Data Protection Act requires that users are made aware of who is tracking them, the purposes for which their personal data will be collected, and whether the data will be sent to a third party, including information about data retention and storage. To sum up, positional data is **"hot"**—you don't want to store it if there is no compelling need to do so.

Geolocation Best Practices (EU)

- **Disable location services settings on the device.**
- **Disable radios when they are not actively in use:** disable BT and turn off Wi-Fi if these capabilities are not needed. Use Airplane Mode when the device is not in use. Ensure BT and Wi-Fi are disabled when Airplane Mode is engaged.
- **Apps should be given as few permissions as possible:**
  - Set privacy settings to ensure apps are not using or sharing location data.
  - Avoid using apps related to location if possible, since these apps inherently expose user location data. If used, location privacy/permission settings for such apps should be set to either not allow location data usage or, at most, allow location data usage only while using the app. Examples of apps that relate to location are maps, compasses, traffic apps, fitness apps, apps for finding local restaurants, and shopping apps.

Geolocation Best Practices (EU)

- **Disable advertising permissions to the greatest extent possible:**
  - Set privacy settings to limit ad tracking, noting that these restrictions are at the vendor's discretion.
  - Reset the advertising ID for the device on a regular basis. At a minimum, this should be on a weekly basis.
- **Turn off settings** (typically known as **FindMy or Find My Device settings**) that allow a lost, stolen, or misplaced device to be tracked.
- **Minimize web-browsing on the device as much as possible**, and set browser privacy/permission location settings to not allow location data usage.
- **Use an anonymizing Virtual Private Network (VPN)** to help obscure location.
- **Minimize** the amount of data with location information that is **stored in the cloud**, if possible.

Geolocation Best Practices (SP)

- ***Use the least precise measurement necessary.*** If your application merely needs to know the city in which the user is currently located, only request this degree of accuracy from the location API. Where “coarse” permissions are available, use these.
- ***Discard data after use.*** Unless data is explicitly needed over an extended period of time, this data should be discarded. This means that either logging subsystems should not receive the data in the first place or they should be immediately expunged. Some companies take the approach of overwriting past positional data immediately when an update is received.
- ***Keep data anonymous.*** If data does need to be retained, ensure that it cannot be associated with other personal data. This includes ensuring that cookies are not used for tracking mechanisms and that requests for location data go over secure channels.

Geolocation Best Practices (SP)

- ***Indicate when tracking is enabled.*** Users should be visually notified that their whereabouts are being recorded. Systems such as the iPhone and Android have dialogs to inform users about this explicitly, either on use or on install. On platforms that don’t have this capability, be sure to notify the user yourself.
- ***Use an opt-in model.*** All software using geolocation data should have this functionality disabled until explicit confirmation from the user. Provide an interface to disable this at any time. Wherever possible, give the user the ability to specify their location manually, as with a ZIP code.
- ***Have a privacy policy.*** Be able to provide guarantees to your users about how you use their positional data, and what you’ll do with it if it’s requested in a civil or criminal case. It’s important to have this ready before a request like this arrives.
- ***Familiarize yourself with local laws.*** Different countries and states have different restrictions and requirements involving tracking information. Ensure that you’re aware of the ones that apply to your target regions.

End of the session