Information Systems and Network Security

Chapter 10

- Security Policies and Measures in Mobile Computing

-Sanket Mohan Pandhare

What is mobile computing?

- Mobile computing is to describe technologies that
  - enable people to access network services anyplace, anytime, and anywhere, with portable and wireless computing and communication devices
  - **Mobile Computing** is a generic term describing the application of small, portable, and wireless computing and communication devices. This includes devices like laptops with wireless LAN technology, mobile phones, wearable computers and Personal Digital Assistants (PDAs) with Bluetooth or IRDA interfaces, and USB flash drives.

- Aspects of mobility
  - User mobility
    - Between different geographical locations
    - Between different networks
    - Between different communication devices
    - Between different applications
  - Device portability
    - Between different geographical locations
    - Between different networks

Applications of mobile computing

- Vehicles
  - transmission of news, road condition, weather, music via Bluetooth
  - personal communication using GSM
  - position via GPS
  - network for vehicles close-by to prevent accidents, guidance system
  - vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance
- Medical
  - Nurses/Doctors in Medical offices are now using Wireless Tablet PCs/WLAN to collect and share patient information.
- Sales
  - Sales representatives are using Tablet PCs with Smart phones for presentation, transmitting/access information among office, hotel, and customer location.
- Emergencies
  - Early transmission of patient data to the hospital, current status, first diagnosis
  - Provide mobile infrastructure in dealing with Natural Disaster (earthquake, hurricane, fire), terrorist attacks, war, ...

Challenges in mobile computing

- Mobility means changes
- Hardware
  - Lighter, smaller, energy management, user interface
- Low bandwidth, high bandwidth variability
  - Kbit/s to Mbit/s, bandwidth fluctuation
- Security risk
  - Devices more vulnerable, endpoint authentication harder
- Heterogeneous network
  - Different devices, interfaces and protocols
- Location awareness
  - Locality adaptation
- Restrictive regulations of frequencies
  - Frequencies have to be coordinated

Bluetooth

- Bluetooth is used to connect and exchange information between devices like PDAs, mobile phones, laptops, PCs, printers and digital cameras wirelessly.
- Low-cost, short range (up to 10m), low power consumption, license-free 2.45 GHz band.
- Using the same frequency range, Bluetooth differs from Wi-Fi in that
  - Different multiplexing schemes.
  - Wi-Fi with higher throughput, greater distances, more expensive hardware, and higher power consumption.
- Applications:
  - Wireless mouse, wireless headset

RFID: Radio Frequency Identification

- RFID is a method of remotely storing and retrieving data using devices called RFID tags.
  - An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product.
  - RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver.
  - No line-of sight required (compared to laser scanners)
  - Withstand difficult environmental conditions (cold, frost etc.)
- Categories:
  - Active RFID: battery powered, distances up to 100 m
  - Passive RFID: operating power comes from the reader over the air, distances up to 6 m
- Applications:
  - Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping

GSM

- Global System for Mobile Communications
- One of the most popular standards for mobile phones in the world.
- GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity.
- One of the key features of GSM is the Subscriber Identity Module (SIM), commonly known as a *SIM card*. The SIM is a detachable smartcard containing the user's subscription information and phonebook.

GPRS

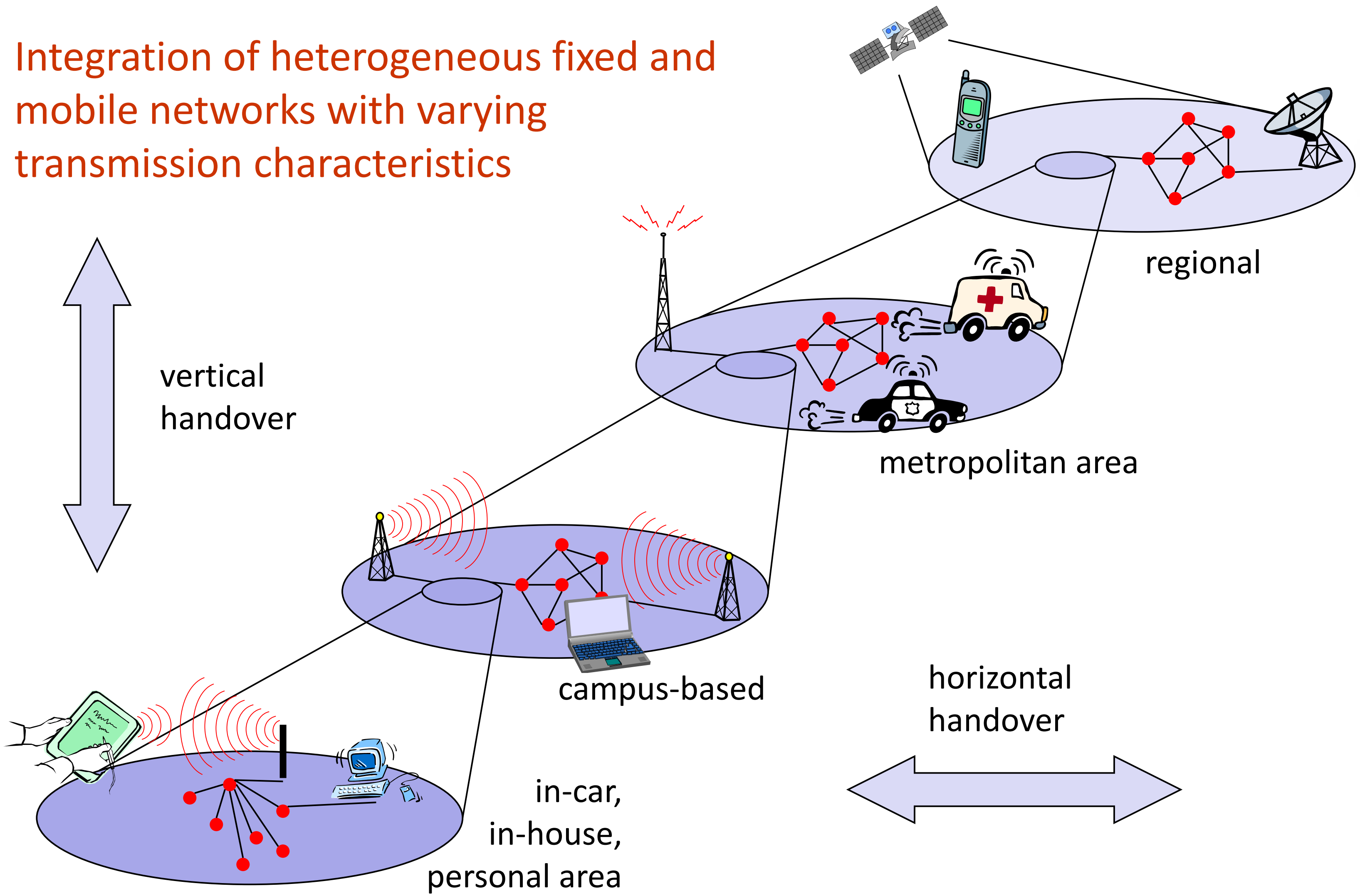
- GPRS: General Packet Radio Service
- It is a mobile data service available to users of GSM mobile phones. It is often described as "2.5G“.
- GPRS is packet-switched which means that multiple users share the same transmission channel, only transmitting when they have data to send.
- GPRS provides moderate speed data transfer, by allocating unused cell bandwidth to transmit data.
  - Poor bit rate in busy cells
  - Usually, GPRS data is billed per kilobytes of information transceived
- In 3G mobile systems like UMTS (Universal Mobile Telecommunication System), voice and data services will be mixed in a normal communication.
- In 4G mobile systems we use VoLTE (Voice over Long-Term Evolution)
- 4G wireless networks typically give you 30 Mbps speeds on mobile devices, 5G speeds can hit anywhere from 60 Mbps to 1,000 Mbps depending on where you are.

PDA

- Personal digital assistants (PDAs or palmtops)
  - handheld devices that were originally designed as personal organizers, but became much more versatile over the years.
  - A basic PDA usually includes a clock, date book, address book, task list, memo pad and a simple calculator.
  - One major advantage of using PDAs is their ability to synchronize data with desktop, notebook and desknote computers.
- The currently major PDA operating systems are:
  - Palm OS by PalmSource, Inc
  - Windows Mobile (Windows CE) by Microsoft
  - BlackBerry by Research In Motion
  - Symbian by a group of companies

Integrated mobile computing

Integration of heterogeneous fixed and mobile networks with varying transmission characteristics



Mobile Threats and Attacks

- Mobile devices make attractive targets:
  - People store much personal info on them: email, calendars, contacts, pictures, etc.
  - Sensitive organizational info too
  - Can fit in pockets, easily lost/stolen
  - Built-in billing system: SMS/MMS (mobile operator), in-app purchases (credit card), etc.
    - Many new devices have near field communications (NFC), used for contactless payments, etc.
    - Your device becomes your credit card
  - Location privacy issues
- NFC-based billing system vulnerabilities

Mobile Device Loss/Theft

- Many mobile devices lost, stolen each year
  - 113 mobile phones lost/stolen every minute in the U.S.
  - 56% of us misplace our mobile phone or laptop each month

Device Malware

- iOS malware: very little
- Juniper Networks: Major increase in Android malware from 2010 to 2018
- Android malware growth keeps increasing ($$$)
- Main categories:
  - Trojans
  - Monitoring apps/spyware
  - Adware
  - Botnets

Location Disclosure

- MAC, Bluetooth Addresses, IMEI, IMSI etc. are globally unique
- Infrastructure based mobile communication
- Peer-to-Peer ad hoc mobile communication

Mobile Access Control

- Very easy for attacker to control a mobile device if he/she has physical access
  - Especially if there’s no way to authenticate user
  - Then device can join botnet, send SMS spam, etc.
- Need access controls for mobile devices
  - Authentication, authorization, accountability
  - Authentication workflow:
    - Request access
    - Supplication (user provides identity, e.g., John Smith)
    - Authentication (system determines user is John)
    - Authorization (system determines what John can/cannot do)

Authentication: Categories

- Authentication generally based on:
  - Something supplicant knows
    - Password/passphrase
    - Unlock pattern
  - Something supplicant has
    - Magnetic key card
    - Smart card
    - Token device
  - Something supplicant is
    - Fingerprint
    - Retina scan

Authentication: Passwords

- Cheapest, easiest form of authentication
- Works well with most applications
- Also the weakest form of access control
    - Lazy users' passwords: *1234*, *password*, *letmein*, etc.
    - Can be defeated using dictionary, brute force attacks
- Requires administrative controls to be effective
    - Minimum length/complexity
    - Password aging
    - Limit failed attempts

Authentication: Smart Cards/ Security Tokens

- More expensive, harder to implement
- Vulnerability: prone to loss or theft
- Very strong when combined with another form of authentication, e.g., a password
- Does not work well in all applications
    - Try carrying a smart card in addition to a mobile device!

Authentication: Biometrics

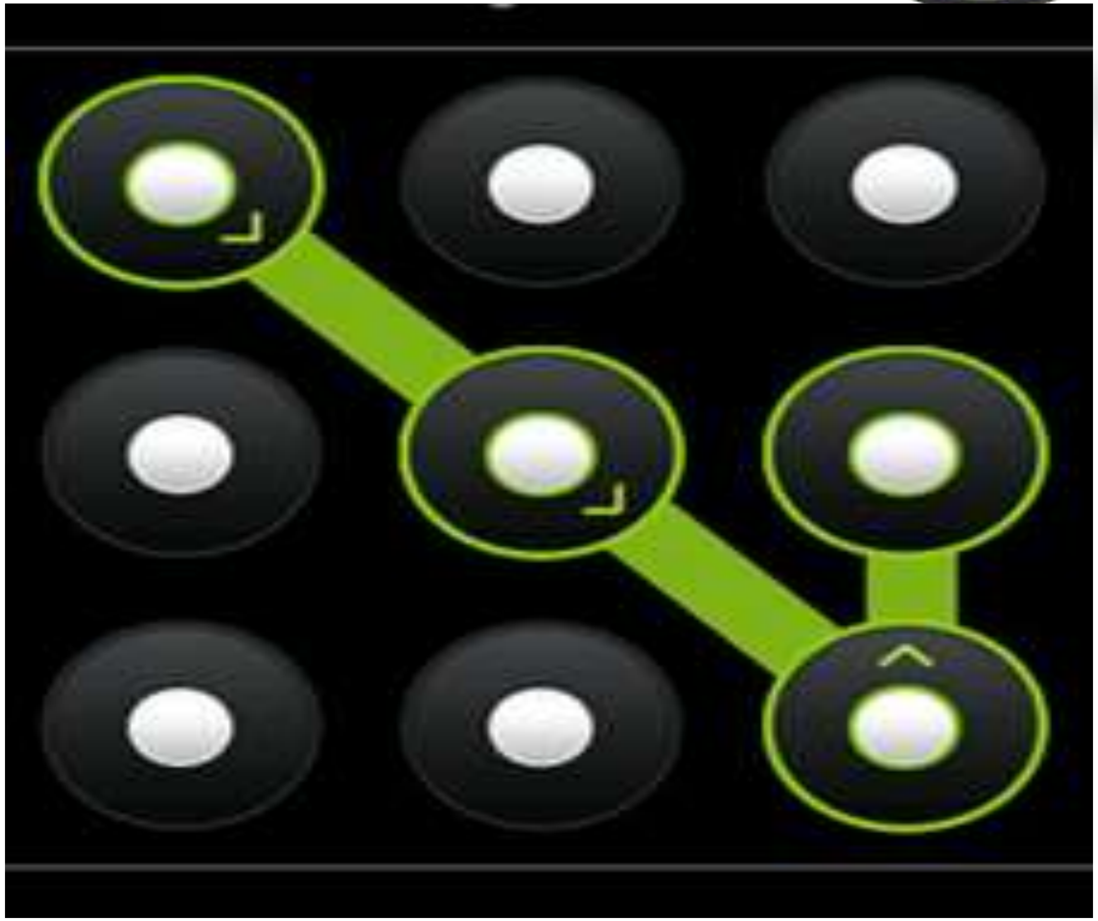
- More expensive/harder to implement
- Prone to error:
  - False negatives: not authenticate authorized user
  - False positives: authenticate unauthorized user
- Strong authentication when it works
- Does not work well in all applications
  - Fingerprint readers becoming more common on mobile devices

Mobile Device Information Leakage

- Types of mobile device information sources:
  - Internal sources (e.g., GPS location, IMEI, etc.)
  - External sources (e.g., Device Trackers, etc.)
- Third-party mobile apps can leak info to external entities
  - Send out device ID (IMEI/EID), contacts, location, etc.
  - Apps ask permission to access such info; users can ignore!
  - Apps can intercept info sent to a source, send to different destination!
- Motives:
  - Monitor employees' activity using accelerometers
  - Ads, market research (include user location, behavior, etc.)
- How do we protect against such information leakage?

Authentication: Pattern Lock

- Swipe path of length
  4–9 on 3 x 3 grid
- Easy to use, suitable for mobile devices
- Problems:
  - 389,112 possible patterns; (456,976 possible patterns for 4-char case-insensitive alphabetic password!)
  - Attacker can see pattern from finger oils on screen



Importance of Security Policies relating to Mobile Computing Devices

- One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices.
- When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure.
- Information classification and handling policy should clearly define what sorts of data may be stored on mobile devices. In the absence of other controls, simply not storing confidential data on at-risk platforms will mitigate the risk of theft or loss.

Operating Guidelines for Implementing Mobile Device Security Policies

- Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.
- Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
- Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
- Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,
- Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized inventory database.

Cont.

- Label the devices and register them with a suitable service that helps recovered devices to the owners.
- Remove data from computing devices that are not in use or before re-assigning those devices to new owners. This is to preclude incidents through which people obtain "old" computing devices that still had confidential company data.
- Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Summary

- Mobile devices are increasingly popular and that’s where we are losing the importance of critical data.
- BYOD (Bring your own device) Trends
- There are many threats and attacks against mobile devices, e.g., loss/theft, sensitive information leakage, and location privacy compromise
- Mobile access control, information leakage protection, and location privacy protection, etc.
- Each and every organization need to have the mobile device security policies to handle the issues related to mobile computing