# CSE 484 / CSE M 584
# Computer Security:
# iOS, Wireless Security & Wireshark

TA: Adrian Sham

adrsham@cs

With material from Franzi and Ben's slides

# Logistics / Reminders

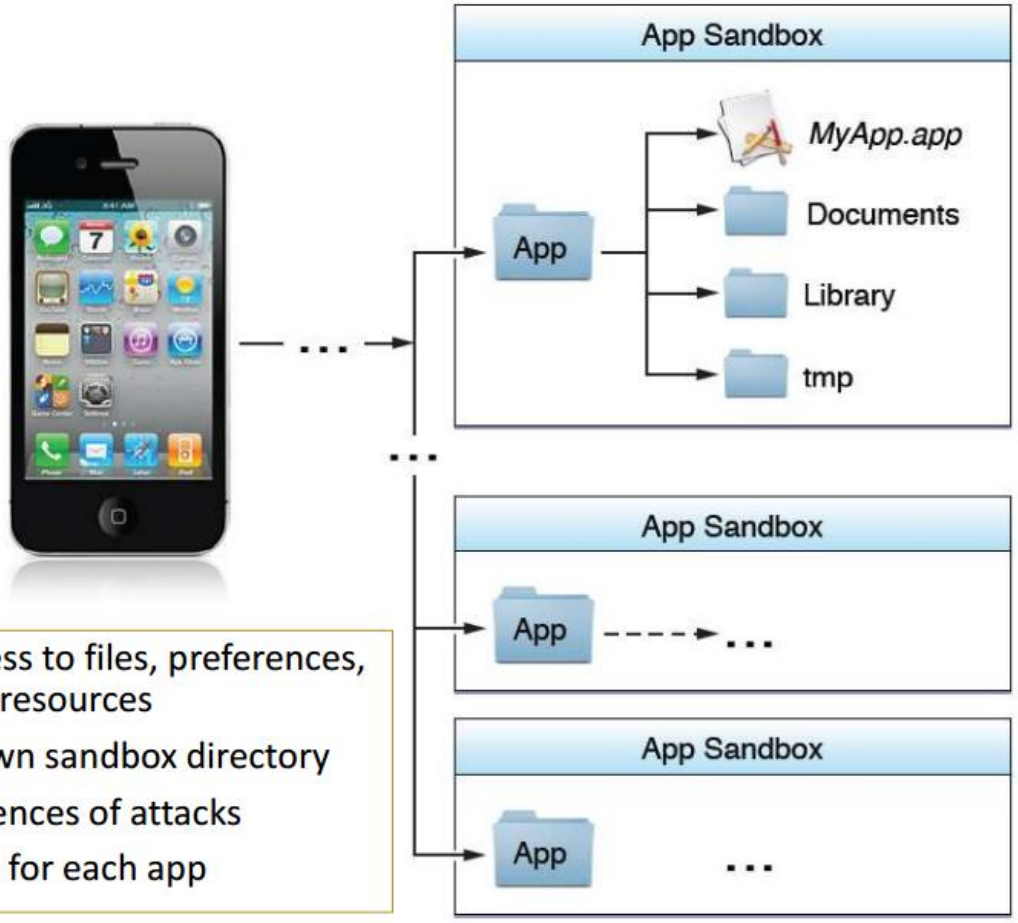
- Tomorrow **Ian** will introduce more tools you will need for Lab #3
- Lab #3 out soon, more info in a bit
- Homework #3 due 5/29, 5pm
- Office hour:
  - Michael and Adrian: 9:30-10:30am, CSE 218
- Today
  - iOS security
  - Networking basics
  - Wireless security
  - Wireshark

# Apple iOS Security

- Device Security
  - Prevent unauthorized use of the device
- Data Security
  - Protect data at rest; device may be lost or stolen
- Network security
  - Networking protocols and encryption of data in transmission
- App security
  - Secure platform foundation

From : http://courses.cs.washington.edu/courses/cse484/14au/slides/LEC16.pdf

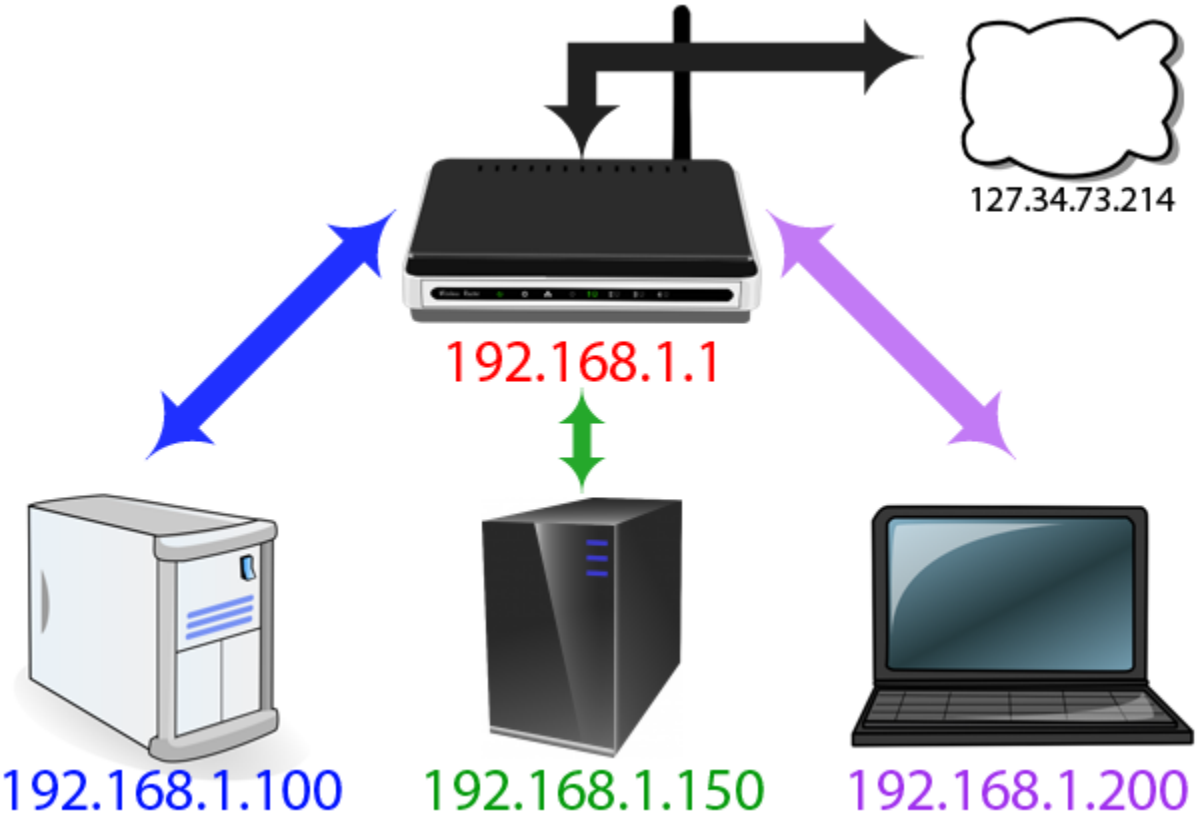
# iOS Sandbox




- Limit app's access to files, preferences, network, other resources
- Each app has own sandbox directory
- Limits consequences of attacks
- Same privileges for each app

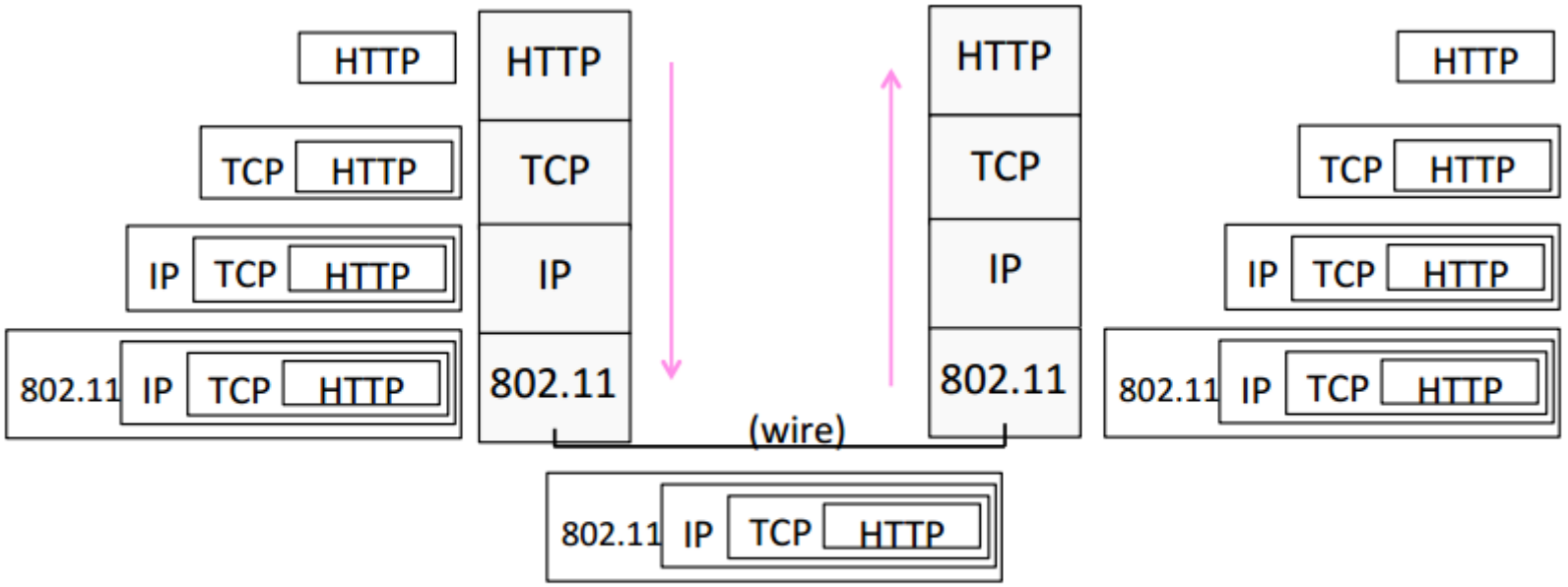
From : http://courses.cs.washington.edu/courses/cse484/14au/slides/LEC16.pdf

# Quick review of networking




http://www.howtogeek.com/66214/how-to-forward-ports-on-your-router/

# Encapsulation



# Terminology

- MAC address: A unique identifier assigned to network interfaces for communications on the physical network segment
- IP address: A numerical label assigned to each device in the network
- FTP: A standard network protocol used to transfer computer files from one host to another over TCP
- Port: A software construct serving as communications endpoint in a computer's host operating system (SSH is port 22)

# Broadcast Nature of WiFi

- Anyone can eavesdrop on wireless communications.
  - Even on some secured networks (e.g., secured with WEP) if eavesdropper is also on network.
- Firesheep: one-click session hijacking
  - http://codebutler.github.com/firesheep/
- Solution: end-to-end encryption (SSL/TLS)

# Lab #3: Network Security Lab

1. Exploring Network Traces
   - Study network traffic using Wireshark, answer questions
2. Anomaly Detection
   - Write a program to identify port scanning
3. Network Attacks (Extra Credit)
   - Crack WEP
   - Decrypt HTTPS connection
   - Recover simulated victim's username and PW

# Wireshark

- Free & open-source network packet analyzer.
- http://www.wireshark.org/
- Documentation http://www.wireshark.org/docs
- Demo
  - Capturing packets
  - Filtering packets
  - Inspecting packets
    - HTTP vs. HTTPS
- Security/Privacy
  - Wireshark allows you to monitor other people's traffic
  - Do NOT use wireshark to violate privacy or security!
- Great slides from CSE 461 here
- A lot of resources online for Wireshark

# Wireshark tips

- Linux install do ‘sudo usermod –a –G wireshark <username>’, re-login
- Color coding
  - Green: TCP
  - Dark Blue: DNS
  - Light Blue: UDP
  - Black: TCP with error
- Filtering packets
  - Capture filter
    - udp
    - Tcp
    - Udp port 53
    - Dst host www.cs.washington.edu
  - Display filter
    - ip.dst == 192.168.1.1
    - http
    - http || arp
    - http && ip.src == 10.0.2.3
    - tcp.port eq 80