WIRELESS NETWORKS: TECHNOLOGY & LEGAL ISSUES

Don Mason
Associate Director

National Center for Justice and the Rule of Law
The University of Mississippi School of Law

SEMINAR OUTLINE:

I. Technology Overview

II. Investigative Considerations

III. Legal and Ethical Issues

QUESTIONS?

Please email your questions, additions, or corrections, at *any* time to:

drmason@olemiss.edu

I. TECHNOLOGY

Several technologies

- Bluetooth
- Infrared
- Cellular/Mobile networks
- Satellite
- Wireless metropolitan area networks
  - IEEE 802.16 standard – "WiMAX"
- Our particular focus here: Wireless LANs
  - IEEE 802.11 standards – "Wi-Fi"

WIRELESS NETWORKS

- Wireless local-area networks ("WLANs"), commonly known as "Wi-Fi" ("wireless fidelity") networks, connect users to the Internet through radio wave frequencies on the unlicensed 2.4 and 5 GHz radio bands.
- Several varieties:
  - Private residences and businesses
  - Hotspots (ex: airports, hotels, coffee shops)

Increasing Ubiquity

- April 2012 study estimated 1 in 4 Internet-connected households in world used wireless home networks.
- Forecast: By end of 2012, 73% of households worldwide with broadband Internet service would be wireless.

Increasing Ubiquity

- Top ten by percentage of households (2012)
  - South Korea – 80.3%
  - United Kingdom – 73.3%
  - Germany – 71.7%
  - France – 71.6%
  - Japan – 68.4%
  - Canada – 67.8%
  - Italy – 61.8%
  - **United States** – 61%
  - Spain – 57.1%
  - Australia – 53.8%

Why a home network?

- Proliferating wireless-enabled devices
  - Computers, laptops, netbooks, tablets, printers, remote storage devices
  - Cell phones, smartphones, digital cameras
  - TV's and streaming video boxes
  - Digital audio players
  - Video game consoles
  - Home security systems, appliances, and more
- Practically mandatory
- Ease of setup

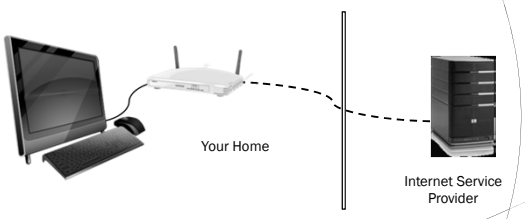
THE BASIC COMPONENTS

Personal Computers

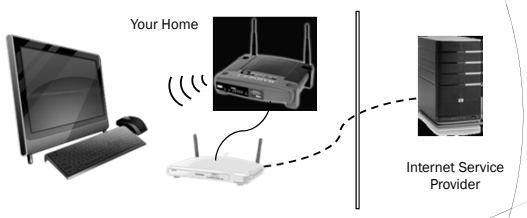
Home computers connect to the Internet in a variety of ways:

- Modems
  - Dial-up, Cable, DSL
- Routers
  - Wireless or Wired

Modem Connection



Routers



Routers

- Home routers may take two forms:
  - Wired – each computer connects to the router with a cable
    - Speeds of 100 Mbps
  - Wireless – computers connect through a signal that is broadcasted by the router
    - Home wireless networks allow sharing of a connection as far as 750 feet
    - Unauthorized access is much easier
    - Speeds up to 600 Mbps (or faster, promised with newest version, 802.11ac)

Routers

- Little computers dedicated to routing network traffic
- Functions
  - "Routing" information between computers, and between computers and the Internet
  - DHCP – Dynamic Host Configuration Protocol – assigning dynamic IP addresses
  - NAT – Network Address Translation – translating IP addresses of packets – in effect, a software Firewall
- Wireless access point (WAP)

IP Addressing

- Each device on the Internet has a unique IP (Internet Protocol) address, such as:
  - 317.23.90.134
- Computers, servers, and even printers have an IP address
- Addresses are usually temporary
  - Temporary addresses are called “dynamic”
  - In some cases, “static” addresses are assigned to a specific computer and do not change

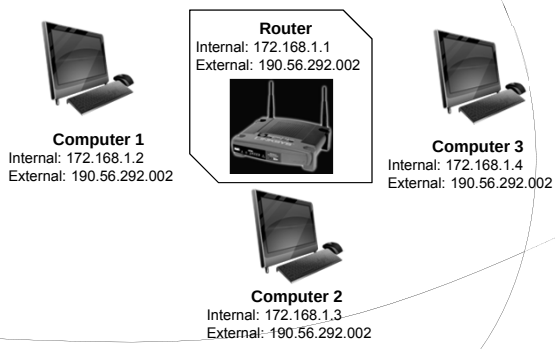
IP Addressing

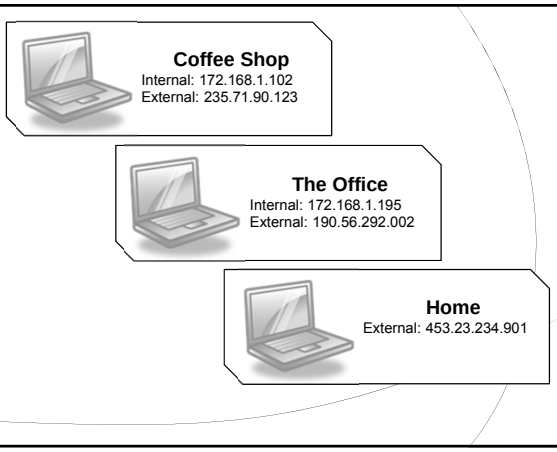
- Some businesses and organizations have a range of IP addresses assigned to them
  - Government agency ranges can easily be found on the Internet
  - Disney, for example, uses 224.0.19.0 - 224.0.19.63
- ISPs also have a range of IP addresses to assign to their users

IP Addressing

- If a network utilizes a router, there are two IP addresses involved
  - **Internal** (local/private): each computer has an internal IP address that distinguishes the computers on the network
  - **External** (Internet): the unique IP address assigned to the router by the ISP
    - Data is received at the external IP address by the router, and then the router sends the information to the correct internally-addressed computer

IP Addressing





Wireless encryption

- Wired Equivalency Privacy (WEP)
  - Easily breakable
- Wi-Fi Protected Access (WPA & WPA2)
- No encryption = *open* wireless access
- Typical default – No security enabled out-of-box

PUBLIC NETWORKS

Public Networks

- Where do public networks exist?
  - McDonalds
  - Starbucks
  - Public Libraries
  - Hotels
  - Apartment Buildings
- Often allow users to connect without providing any information that reveals their identity

Public Networks

- How safe are they?
  - Not very!
  - Wi-Fi hotspots major security risks
  - Easy-to-find tools allow other users to obtain all of your account information and browsing history
  - The provider may even track it intentionally for research purposes

Public Networks

Public Networks

Public Networks

- *Pineapple*
- $90-$100
- Intercepts Wi-Fi traffic
- "Man-in-the-middle"

Public Networks

- Precautions
  - Only connect to secure hotspots
    - Beware if no password is required
  - Be sure your security is up to date
  - Use a Virtual Private Network (VPN)
  - Encrypt your sensitive data
  - Vary and strengthen your passwords
  - Stay with secure (HTTPS) sites if possible
  - Avoid sending private information if possible
  - Turn off your Wi-Fi when not using it
  - Consider using your cellular network instead

EXPANSION

- Some cities have sought to provide free public Wi-Fi access.
- Some websites document maps of thousands of hotspots within a city.

TO Wi-Fi OR NOT TO Wi-Fi

- Unauthorized use of Wi-Fi signals is becoming commonplace in many parts of the country

PROS AND CONS OF Wi-Fi

Pros:

- Convenient
- Mobile (no need to get tied up with cords)
- Installation costs are reasonable
- Hotspots often free
- Helps protect against exceeding mobile data caps
- Higher speeds than mobile

PROS AND CONS OF Wi-Fi

Cons

- Not the same level of security and privacy as a hard-wired local area network
- May not be as secure as cellular
- May have to enter username and password
- May have to enter payment information

Trend

- Toward convergence of 3G/ 4G cellular and public Wi-Fi
  - Public Wi-Fi networks could become part of cellular provider networks
- Obvious benefits
  - Easier access to Wi-Fi
  - Better network coverage
  - Increased capacity (e.g., in stadiums)
  - Faster speeds

II. INVESTIGATIVE CONSIDERATIONS

Challenges

- Diversity of devices
- Evidence collection
  - Don't forget to look for remote devices
- Evidence preservation
  - Possibility of remote access to damage or destroy evidence
- Ease of unauthorized access
- Public networks

Public Networks

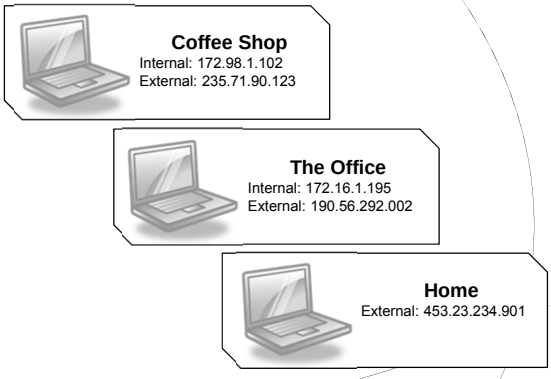
- More than anything, they make people feel like their actions are anonymous
- Beyond tracking from others on the network at the time, use of public networks does make it difficult to track actions back to the user

IP Tracking

- Since every computer has a unique address, actions on the Internet can [somewhat] easily be traced back to the user.
  - A range of IP addresses is assigned to ISPs. If given a certain IP address, the ISP can be easily determined.
  - The ISP can track the IP address to the account holder at a designated time.

IP Tracking

- One important thing to remember – ISPs are not required to keep such data.
  - Some ISPs may delete such information after only 3 days.
  - Congress has considered such a requirement, but has yet to pass one.



MAC Addresses

- While an IP address is assigned by a network, each computer also has a unique MAC (Machine Access Control) address assigned by the computer's (actually the network interface's) manufacturer
  - IP = software
  - MAC = hardware
- Like a unique serial number. Example:
  - 70-F3-95-38-1F-06

Beyond our immediate scope

- Using tools to detect wireless networks and/or to sniff packets
- "Interrogating" routers

Routers – Wireless Access Points

- Advertise/Broadcast their names (SSIDs – service set identifiers), presence, and capabilities
- Both volatile and non-volatile evidence
- Can send logs over network to *remote* storage

Routers – WAPs

- Volatile evidence that *may* be found:
  - DHCP assignments
  - History of connections by MAC addresses
  - List of IPs associated with MACs
  - Logs of wireless events (access requests, etc.)
  - History of client signal strength
  - Routing tables
  - Access control lists
  - Etc.

III. LEGAL ISSUES

New crimes (?)

- "Wardriving" (or "war chalking") ??
- "Piggybacking"
  - Unauthorized access to computer network
  - "Theft of telecommunications" (Canada)
- Failure to secure network
  - Actionable negligence?
- Giving Wi-Fi network a harassing or racist name
- "Evil twin" data thefts

Defenses

- Accident / Mistake
- Pop-ups
- SODDI
- Computer Virus or other malware
- Remote Access
- Wireless Access
- Worm
- Rootkit
- Virtual Images

Open Wireless

April 18, 2007 6:00 AM PDT

Police blotter: Open Wi-Fi blamed in child porn case

By Declan McCullagh
Staff Writer, CNET News

19 comments

Related Stories

Police blotter: Sensual masseuse sues ex-customer
April 11, 2007

Police blotter is a weekly News.com report on the intersection of technology and the law.

What: A Texas man, whose home is raided in search of child porn, points to an open Wi-Fi connection that is not password-protected. He is convicted of possession of child pornography but appeals the decision, asserting an invalid search warrant.

Open Wireless Defense

- Wireless Internet allows users to broadcast their Internet connections
- Many wireless routers and access points do not have encryption and security settings turned on by default
- "War driving" and other issues can result if users leave wireless Internet connections open

Open Wireless

- Forensic Considerations:
  - Some WiFi routers and access points will log connections (generally not by default)
  - Investigators should check for presence of wireless Internet devices
  - SSID name and encryption settings should also be checked

Open Wireless

- Forensic Considerations:
  - Police WiFi devices should be disabled during consent searches or warrant executions
  - War driving will lead investigators to IP address of the Internet connection, not to the actual suspect's computer
  - The MAC (Media Access Control) address of the suspect computer may be in logs in the wireless router
  - If suspect computer is found it may have the SSID name of WiFi hotspots in the registry

Open Wireless

- What is the context?
  - Does user have a firewall?
    - Was it in place?
  - Are the suspect images always placed on the computer when the person is at the console?
    - Browser patterning?

Key Considerations

- Most technical defenses can be refuted by computer forensics
- Was Def at the computer when the crime was committed?
- Is there evidence suggesting that Def had knowledge and/or intent?
- Requires thorough time/date analysis of computer and real world events

52

Wiretap Act

- Is sniffing open Wi-Fi wiretapping?
- *POSSIBLY*
  - *In re Google Inc. Street View Electronic Communications Litigation*, No. C 10-MD-02184 JW (N.D. Cal. 2011)
- *NO*
  - *In re Innovatio IP Ventures, LLC Patent Litigation*, No. 11 C 9308 (N.D. Ill. 2012)

Fourth Amendment

- Is accessing a shared library via an open wireless network a "search"?
  - *United States v. Ahrndt*, 2010 WL 373994 (D.Or. 2010) ("*Ahrndt I*")
  - *United States v. Ahrndt*, 475 F. App'x 656, 2012 U.S. App. LEXIS 6976 (9th Cir. 2012), *unpublished* ("*Ahrndt II*")
  - *United States v. Ahrndt*, 2013 WL 179326 (D.Or. 2013)

Obtaining evidence w/o a warrant

- Detecting wireless signals while in driveway
  - Curtilage invasion?
- Wireless survey of Wi-Fi signals, regardless
  - *Kyllo v. United States* (2001) problem?
    - *United States v. Sayer*, 2012 WL 2180577 (D. Maine 2012)
      (Router in house across the street)

Challenges to SW affidavits

- *Franks (v. Delaware)* challenges
- Examples*:*
  - *United States v. McGlown*, 2013 WL 2149691 (S.D. Ohio May 2013)
  - *United States v. Stanley*, 2012 WL 5512987 (W.D. Pa. Nov 2012)
  - *United States v. Thomas*, 2012 WL 4892850 (D. Vt. Oct 2012)
  - *United States v. Sayer*, 2012 WL 2180577 (D. Maine June 2012)
  - *United States v. Massey*, 2009 WL 3762322 (E.D. Mo. 2009)
  - *United States v. Klynsma*, 2009 WL 3147790 (D. SD 2009)

Recall requisites

- Given presumption of validity re SW affidavit,
- To obtain *Franks* hearing, Def must make substantial preliminary showing that affiant knowingly or intentionally or with reckless disregard for the truth included a *false statement* that was *necessary to* the finding of probable cause
- *Or* that …

Recall requisites

- The affiant deliberately or recklessly *omitted* "*material" information* which, if supplied,
- *Would negate* the finding of probable cause.

- Significant burdens of production and proof, as Def must show at any hearing, by preponderance, that statements or omissions were intentional or reckless.

AN ATTORNEY'S SPECIAL DUTIES?

- Does an attorney violate the duties of confidentiality and competence when using an unsecured network to communicate client information?

FACTORS FOR TECHNOLOGY USE

1. The ability to assess the level of security.
2. The legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information.
3. The sensitivity of the information.
4. The impact on the client of a possible inadvertent disclosure of privileged or confidential information or work product have, including a possible waiver of the privileges.
5. The urgency (i.e., if it is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, then it may be reasonable in limited cases for an attorney to do so without taking additional precautions)
6. The client's instructions to not use certain technology due to security concerns

See California Bar Formal Op. 2010-179 (2010)

QUESTIONS?

662-915-6898
drmason@olemiss.edu
www.ncjrl.org

CONCLUSION

- Thanks for attending
- Next:
  - *Web Browsing 101*
    - June 25
  - *Hiding Tracks on the Net*
    - August TBD
  - *Mobile Devices*
    - September
  - *Developments in Search & Seizure Affecting ICAC Investigations*
    - October