WIRELESS NETWORKS SECURITY

Shambhu Upadhyaya
Computer Science & Eng.
University at Buffalo
Buffalo, New York 14260

Acknowledgments

- DoD Capacity Building Grant
- NSF Capacity Building Grant
- Cisco Equipment Grant
- Anusha Iyer, Pavan Rudravaram, Himabindu Challapalli, Parag Jain, Mohit Virendra, Chris Crawford, Ameya Sanzgiri

Motivation

- Military
  - Success of Desert Storm in Gulf War attributed to Wireless communication
  - Military superiority may not win war anymore
  - Mass destruction possible with Cyber weapons
  - Data sharing is critical in coalition partners
  - Wireless is key for communication in the intelligence community
- Public/Private
  - Today, a large no. of Internet connections happen from mobile devices
  - Wireless is ubiquitous, it has stayed here
- Info. must flow in and out of government to private sectors

Wireless – Another Perspective

- Why and when of Wireless
  - No way to run the cable
  - Convenience of less hardware – e.g., Conferences
  - Temporary setups
  - Costs of cabling too expensive
  - Scalability and Flexibility - Easy to grow
  - Reduced cost of ownership - initial costs the same as the wired networks
  - Mobility

Mobility and Security

- Increased mobility has become way of life
- Wireless is at the first and last miles
- Presents itself to security problems
- Proper security must be practiced
- A new security culture needs to emerge across the entire Internet user community
- Hacker ethic "destructiveness is inquisitiveness" – must be resisted
- Instead, proper online security habits must be practiced

Good Security Thinking (Edney & Arbaugh '04)

- Don't talk to anyone you don't know
- Accept nothing without a guarantee
- Treat everyone as enemy until proven otherwise
- Don't trust your friends for long
- Use well-tried solutions
- Watch the ground you are standing on for cracks
- Good habits
  - Changing passwords, disconnecting when not in use, run antivirus daily, change default password, use appropriate security and encryption services

Wireless Security – the Course

- An approach of best business practice due to the nature of the topic
- Components of the course
  - Threat model
  - Security protocol
  - Keys and passwords
  - Key entropy
  - Authentication
  - Authorization
  - Encryption

Why is Wireless Different

- First know the distinction between communication and computing (cellular networks vs. data networks)
- Wireless – info. travels through free-space on certain spectrum allocations
- PDAs, Cell phones, pagers inherently less secure
  - Limited bandwidth, memory, processing capabilities
  - Anyone with some technology can intercept it
  - Enemy need not come to you, victims go to attackers simply by roaming
  - Poor authenticating services – poor identity guarantees on user and devices
  - You can deny your act (non-repudiation)
  - Reestablishing connections without re-authenticating is dangerous
- Man in the middle attacks are easier

Security and Privacy

- Wireless infrastructure
  - Less physical assets to protect
  - But there is no locked door on the airways
- Infrastructure protection
  - In Government hands
  - Being public asset, government feels responsible
  - National security
- Military is often the originator of digital security measures
- Regulations are likely to thwart privacy
- FBI's Carnivore program – automated snooping tool, unpopular
  - Similar to wiretapping, but sniff email, designed in 1999
  - Violated free speech and civil rights?
  - Program abandoned completely in Jan. 2005
- NSA's Prism Program
  - Clandestine mass electronic surveillance data mining program (2007)
  - Existence was leaked by Edward Snowden in June 2013

Course Outline

- Mixture of basic and advanced topics
- Projects, Homeworks and Research Reading
- Form groups of 2
- Two midterms (3/28, 5/7) and several quizzes
- Several projects using network simulation tools and laptops

Sample Projects

- Packet Analysis & Spoofing
  - WildPacket's AiroPeek, Ethereal, etc.
- RF Jamming & Data Flooding
  - Get an idea on AP vulnerabilities
- Information Theft
  - Implement a covert channel through a wireless communication path, how easy or difficult?
- Layered Wireless Security
  - Lightweight Extensible Authentication Protocol (LEAP) system of Cisco
- Wireless Bridging Security
  - Fragile communication path from a wireless to wired device

Wireless Networks

- Cellular Networks (CDMA, OFDMA, GSM)
  - 1G, 2G, 3G, 4G, 5G
  - Main function is to send voice (make calls), but data over voice applications (GPRS, EDGE, HSDPA) have been developed to enable web surfing from cell phones
- Data Networks (802.11, 802.15, 802.16, 802.20 - Mobile Broadband Wireless Access (MBWA))
  - Main function is to send data, but voice over data applications have also been developed (e.g., VOIP)
- Emphasis of the course is on Data Networks
  - 802.11: WLANs, MANETs, Sensor Networks
  - 802.11 is a STANDARD with different implementations
  - 802.11 only tells about how to access the channel, how to back-off to prevent collisions, how to send a packet over the air

Cellular Networks

- 1G or first generation
  - analog networks
    - Low voice quality
    - very less security
    - low capacity
- 2G or second generation
  - analog and digital networks
  - Advanced Mobile Phone Service (AMPS)
  - Time Division Multiple Access (TDMA)
  - Global System for Mobile Communications (GSM)
  - Code Division Multiple Access (CDMA)
    - digital encoding
    - high bit rate voice
    - better security
    - limited data communication

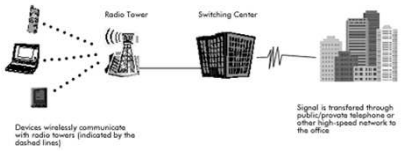
Cellular Networks (Contd.)

- 3G or third generation
  - Includes GSM, EDGE, UMTS, and CDMA2000
  - Universal Mobile Telecommunications System (UMTS)
    - higher data rates
    - more security
    - Transfer rates 26x faster than CDMA networks
  - 3G networks - implemented in the United States in the last 10-12 years
    - AT&T iPhone
- 4G
  - Aims to provide ultra-broadband (gigabit-speed) Internet access to mobile as well as stationary users
  - 100 Mbit/s to 1 Gbit/s

Cellular Networks (Contd.)

- Wireless Wide Area Networks
- Connects to the office network wirelessly from home or while traveling
- Use Radio waves
- Request for information is sent to WAP gateway
- Coverage area - several miles
- Transfer speeds: from 5 kbps - 20 kbps
- Operated by public carriers
- Use open standards such as AMPS, GSM, TDMA, and CDMA

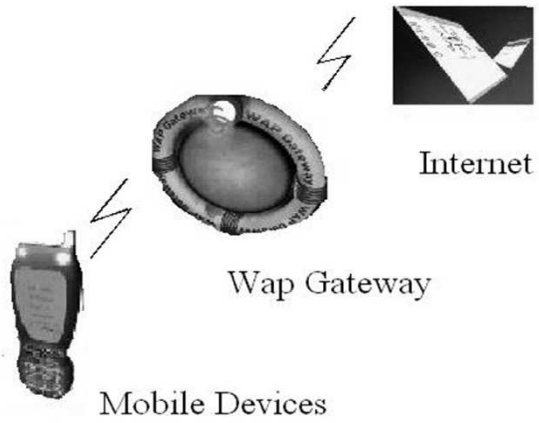
WWAN-Wireless Wide Area Networks



WAP

- WAP - Internet and advanced telephony services
- WAP bridges mobile world, Internet and corporate intranets
- WAP defines WAE (wireless application environment)
  - Micro browser
  - Scripting facilities
  - e-mail
  - World Wide Web (WWW)–to-mobile-handset messaging
  - Mobile-to-telefax access, etc.

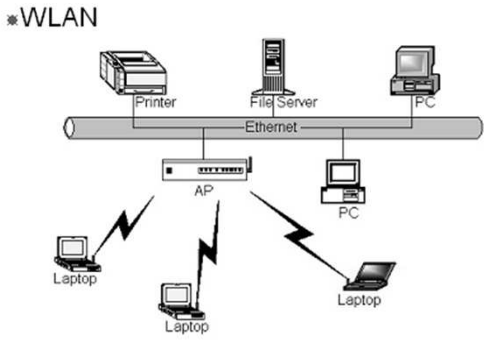
WAP



Data Networks (WLANS)

- WLANs
- Coverage areas-fixed
- Range: 100 - 500 ft - indoors; 1000 ft - outdoors
- Transfer speeds: up to 54 mbps
- Electromagnetic waves-Spread spectrum technology
- As Ethernet is for wired LANs - 802.11 is for wireless LANs
- 802.11 works in unlicensed spectrum of 2.4 GHz

WLAN-Configuration



Wi-Fi-802.11

- Uses unlicensed spectrum - 2.4 GHz
- Simple, flexible, cost effective
- Covers MAC layer and physical layer
- Uses FHSS for transmission
- 802.11b uses DFSS for transmission
- Speeds
  - 2, 9, 11, 54 Mbps
  - Speed depends on
    - Modulation technique
    - Distance of the node to the Access Point
    - FEC level (Forward Error Correction)

802.11 (Contd.)

- MAC (Media Access)
  - Same in 802.11, 802.11b, 802.11a
  - Based on CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)
    - Basic idea
      - RTS (request to send)
      - CTS (clear to send) channel reservation mechanism
- HIPERLAN – Alternative to 802.11, did not survive due to complexity of implementation
- MMAC –HiSWAN – costlier multimedia alternative
- Disadvantage:
  - Cannot provide QoS support for increasing number of multimedia applications

History of 802.11x

- 1990 - IEEE Started 802.11 standard
- 1997 - Drafted 802.11
- 1999 – Drafted 802.11a and 802.11b
- 2003 - 802.11g Draft Approved
- 2006 - 802.11n (draft, ratified in 2009)
- (2003 - 802.15 Draft Approved)
  - Personal Area Networks
  - Bluetooth, ZigBee (low-powered digital radios), etc.

Wireless Network Types

- Fixed networks
  - Point-to-point network
- Nomadic networks
  - Point-to-multipoint network
  - Computing devices are somewhat mobile
  - 802.11b, 802.11g, 802.11a support this
  - Becoming quite commonplace – coffee shop
- Mobile networks
  - Must support high velocity mobility
  - 802.16e, 802.20 and CDMA2000 standards

802.11 Variations

Variation	Operating Frequency	Bandwidth	Disadvantages
802.11	2.4GHz	2 Mbps	Less Bandwidth
802.11b	2.4 GHz	11 Mbps	Lack of QoS and multimedia support
802.11g	2.4 GHz	20 Mbps	Same as 802.11b
802.11a	5 GHz	54 Mbps	More Expensive and less range
802.11h	5 GHz	54 Mbps	Same as 802.11a
802.11n	2.4 GHz or 5 GHz	300 Mbps	Expensive
802.11e	QoS Support to 802.11 LAN		
802.11f	access point communications among multiple vendors		
802.11i	Enhance security and authentication mechanism for 802.11 mac		

Other Types of Data Networks (WLANs)

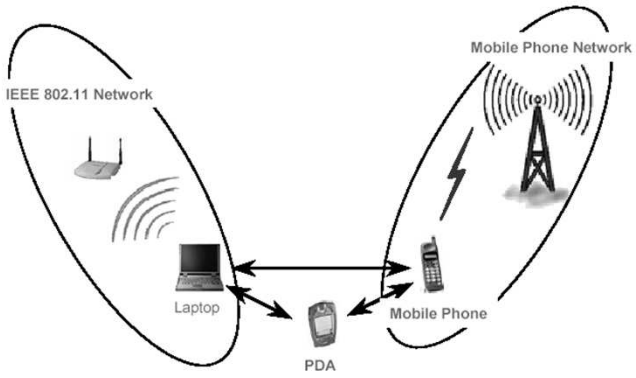
- **HiperLAN**-
  - **H**igh **Per**formance **L**ocal **A**rea **N**etwork
  - Similar to 802.11
  - Two types
    - HiperLAN 1 -20 mbps
    - HiperLAN 2 -54mbps
  - 5Ghz bandwidth
  - One of the prime features of HiperLAN is its support for Wireless ATM
  - WATM - extension of ATM capabilities

- **HomeRF**-
  - Wireless home networking
  - 50 meters
  - Data rates upto 1.6 Mbps
  - Uses SWAP (shared wireless access protocol)
  - Uses 2.4Ghz band

Bluetooth

- Cable replacement technology
- Interconnect portable devices
- 2.45 Gigahertz (GHz)
- Transfer speeds: up to 1 mbps
- Ad hoc network provides spontaneous connectivity
- Range: 20-350 feet
- Supports up to three simultaneous voice channels
- Employs frequency-hopping schemes
- Power reduction to reduce interference
- IEEE 802.15 (standardized within the 802.15 Personal Area Network Working group)

Bluetooth



Bluetooth (Cont..)

- Uses Link Manager Protocol (LMP)
  - To configure
  - Authenticate
  - Handle connections
- Piconets-
  - Up to 8 devices
  - Master and slaves
- Scatternet – up to 10 piconets
- Present status of the technology
  - common with phones and handheld devices
  - Laptops and smartphones are nowadays Bluetooth enabled

Near Field Communication (NFC)

- This is an extension of RFID technology, allowing for two-way communication
- Standard for smartphones to communicate with each other using radio (standardized in 2004)
- Uses
  - NFC is predominantly meant more for secure transactions – Contactless payments, airline check-ins, etc.
  - Social networking – sharing photos, videos, files, etc., securely
  - In-vehicle networks
- Range is a few centimeters
- Logo:

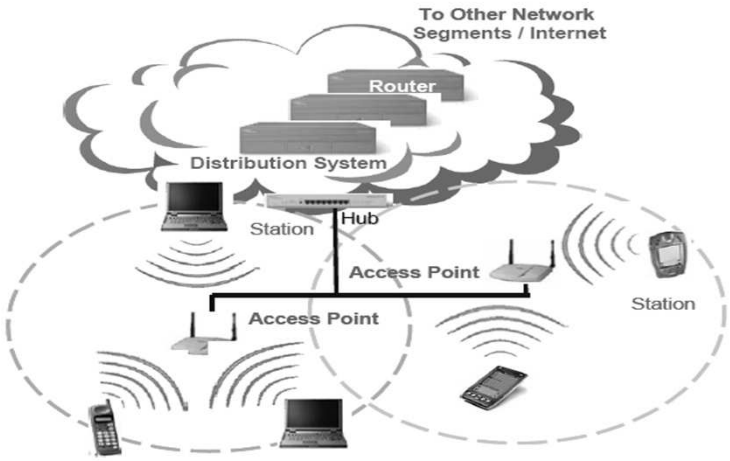

Wireless Networks Deployment Strategies

- Two modes of operation of 802.11 devices
  a) Infrastructure mode
  b) Ad hoc mode
- Infrastructure mode
  - AP bridging wireless media to wired media
  - AP handles station authentication and association to the wireless network
- Ad hoc mode
  - An ad hoc network between two or more wireless devices without Access point (AP)

Infrastructure Mode

- 802.11 networking framework
- Devices communicate through an Access Point (AP)
- AP connected to wired network and a set of wireless stations - Basic Service Set (BSS)
- Extended Service Set (ESS) is a set of two or more BSSes
- Operate in infrastructure mode when required access to the wired LAN
- Corporate sector implementation

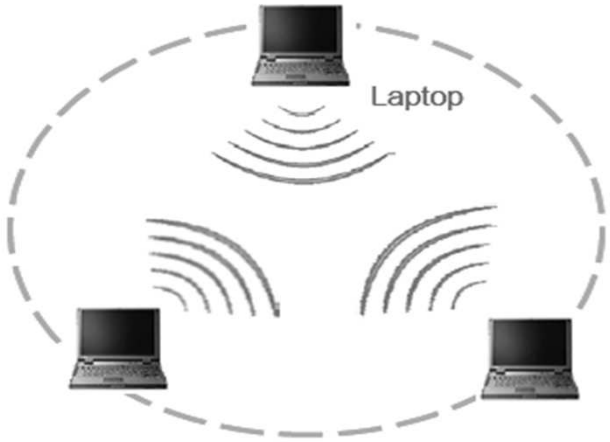
Infrastructure Mode Architecture



Ad-hoc Networks

- 802.11 networking framework
- Devices or stations communicate directly with each other
- Networks with no fixed infrastructure
- Mobile nodes: communicate within radio-range directly
- Node mobility-frequent change in network topology
- Rapidly deployed networks
- Relatively low cost
- The lack of infrastructure
  - Introduces vulnerability to DoS
  - Mobility induces link breakage and channel errors
- Growing commercial and military deployments - rapid need for scalability

Ad-hoc Mode Architecture



Devices Associated with Wireless Networking

- Access point
- NIC compatible devices –
  - Laptops
  - PDAs
  - Scratchpads
- Smart phones-Cellular phones
- Mouse
- Keyboards
- Text messaging devices
- Speakers/Headphones

Wireless Network Concerns

- Radio Signal Interference
  - Sources-Atmospheric noise, Nearby wireless devices
  - Effects-Delay, Blocking, Bit errors, Limit the coverage area
  - Counter measures-Limit operating power, Spread spectrum techniques, Frequency management
- Power Management
  - Battery weight, operation time
- System Interoperability
  - Protocols and Electrical characteristics
- Network Security and threats
  - Main concerns
- Connection Problems
- Installation Issues - Infrastructure, initial installations

Limitations of Wireless Networks

Wireless Devices

- Slow processing power
- Less memory
- Power constraints
- Smaller displays
- Weak authentication

Wireless Networks

- Less bandwidth
- Higher latency
- Lower stability
- Lower availability
- Slow connections

Security Issues in 802.11

- WEP (Wired Equivalent Privacy)
- 128-bit key in 802.11a
- Security Problems - 802.11 family faces the same problems
  - Sniffing and War driving
  - WEP (Wired Equivalent Privacy)
  - Authentication
  - MAC Address
- Default installation
  - Allows any wireless node (NIC) to access the network
  - Walk around and gain access to the network