CSE 707: Wireless Networks Security – Principles and Practices

Shambhu Upadhyaya

Computer Science and Engineering

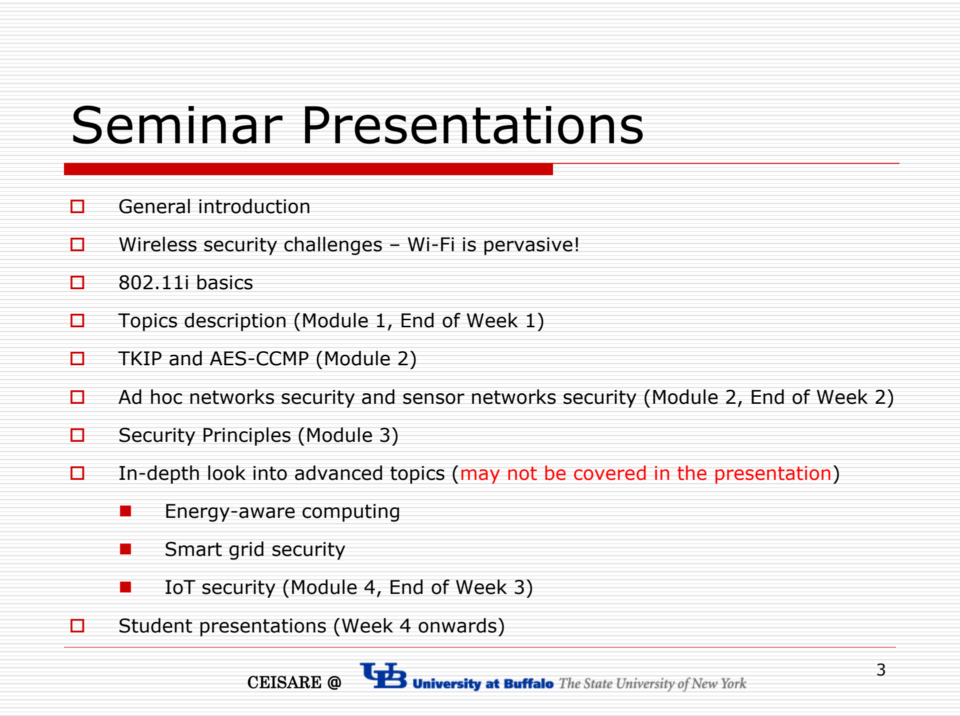
University at Buffalo

Introduction

August 30, 2023

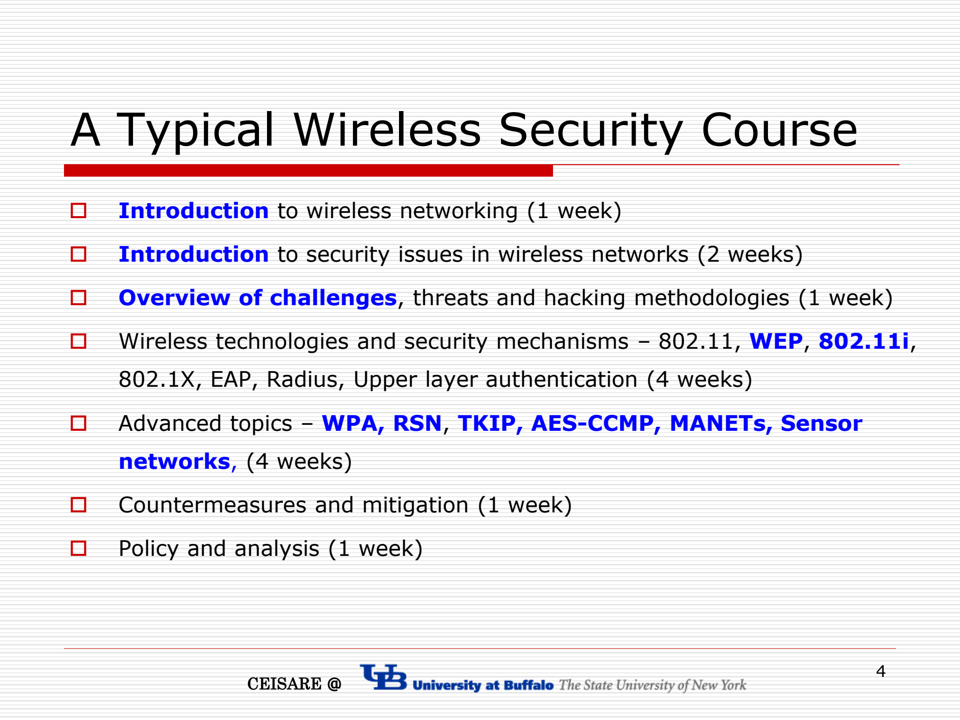
Acknowledgments

- □ DoD Capacity Building Grant
- □ NSF Capacity Building Grant
- □ Cisco Equipment Grant
- □ Anusha Iyer, Pavan Rudravaram, Himabindu Challapalli, Parag Jain, Mohit Virendra, Sunu Mathew, Murtuza Jadliwala, Madhu Chandrasekaran, Chris Crawford, Ameya Sanzgiri, Tamal Biswas (former students)



Seminar Presentations

- □ General introduction
- □ Wireless security challenges – Wi-Fi is pervasive!
- □ 802.11i basics
- □ Topics description (Module 1, End of Week 1)
- □ TKIP and AES-CCMP (Module 2)
- □ Ad hoc networks security and sensor networks security (Module 2, End of Week 2)
- □ Security Principles (Module 3)
- □ In-depth look into advanced topics (may not be covered in the presentation)
  - Energy-aware computing
  - Smart grid security
  - IoT security (Module 4, End of Week 3)
- □ Student presentations (Week 4 onwards)



A Typical Wireless Security Course

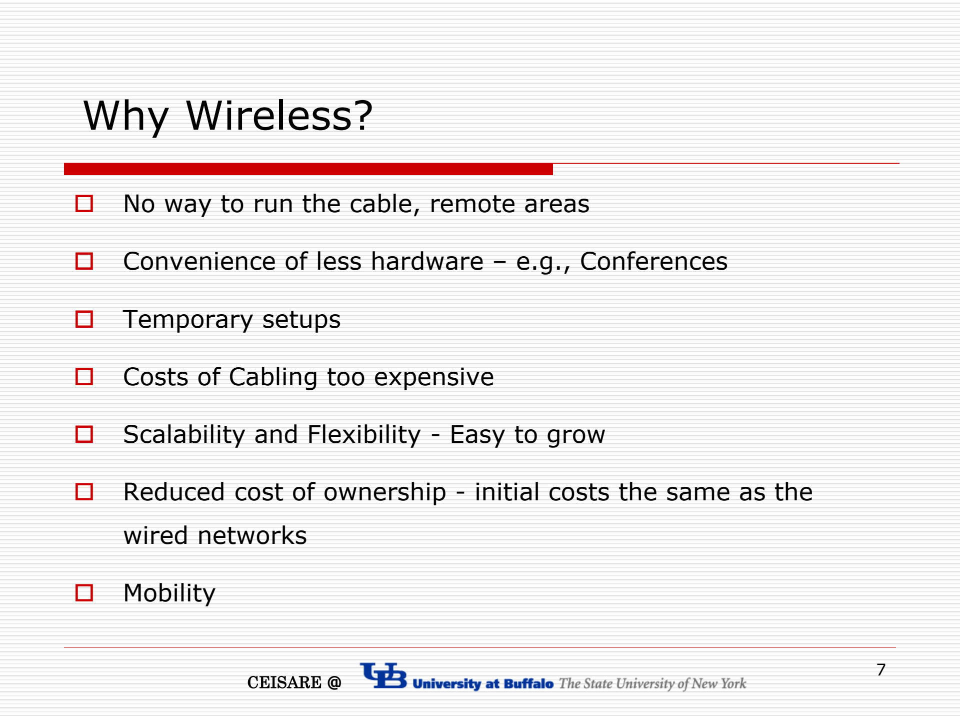
- □ **Introduction** to wireless networking (1 week)
- □ **Introduction** to security issues in wireless networks (2 weeks)
- □ **Overview of challenges**, threats and hacking methodologies (1 week)
- □ Wireless technologies and security mechanisms – 802.11, **WEP**, **802.11i**, 802.1X, EAP, Radius, Upper layer authentication (4 weeks)
- □ Advanced topics – **WPA, RSN**, **TKIP, AES-CCMP, MANETs, Sensor networks,** (4 weeks)
- □ Countermeasures and mitigation (1 week)
- □ Policy and analysis (1 week)

Seminar Course Grading

- Prerequisites
  - A course on Computer Networks and basic knowledge of computer security
  - Some programming experience is essential
- Course webpage
  - http://www.cse.buffalo.edu/faculty/shambhu/cse70723/
- Grading
  - Presentations
  - Research, Projects, any term papers
  - Research round table at the end of the course
  - Attendance mandatory

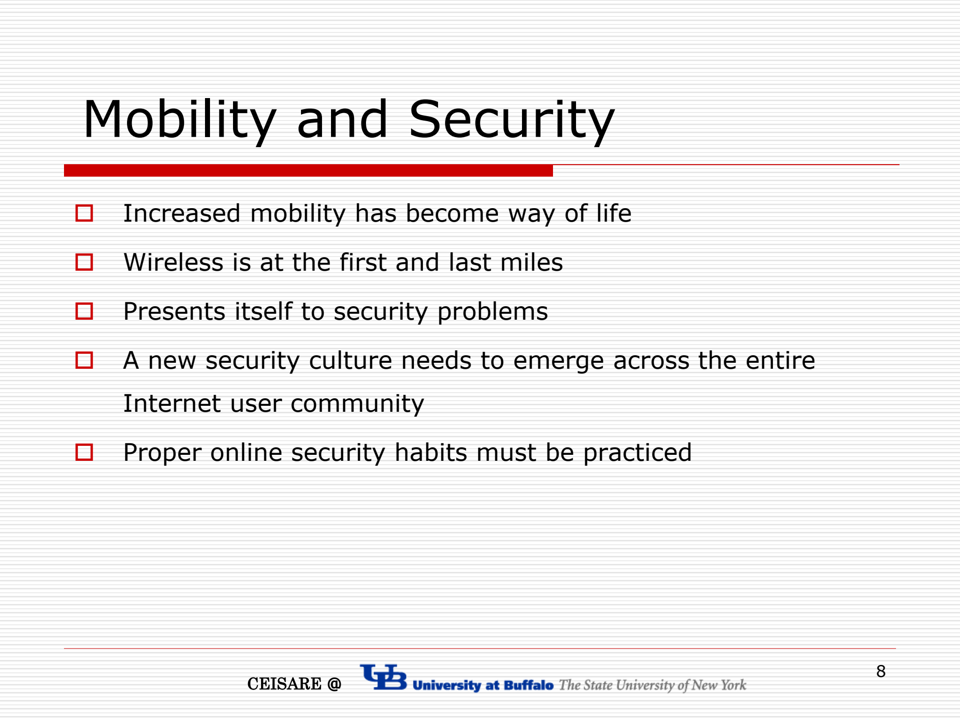
Lab Projects (Hands-on)

- Setting up wireless networks with hybrid technology (not practical this year)
- Setting up multi-hop networks in the lab (not practical this year)
- Packet Analysis & Spoofing
  - WildPacket’s AiroPeek, Ethereal/Wireshark, etc.
- RF Jamming & Data Flooding, DOS attacks
  - Get an idea on AP vulnerabilities, iPhones
- 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
- Key Management
  - Authentication, confidentiality
- Network survivability
  - Admission control, graceful migration, etc.



Why Wireless?

- □ No way to run the cable, remote areas
- □ 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
- □ A new security culture needs to emerge across the entire Internet user community
- □ Proper online security habits must be practiced

What Would Constitute a Typical Wireless Security Course

- Components of the course
  - Threat model
  - Security protocol
  - Keys and passwords
  - Key entropy
  - Authentication
  - Authorization
  - Encryption
  - Trust issues
  - Detection models

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

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 (WAP, GPRS) have been developed to enable web surfing from cell phones
- Data Networks – 802.11, 802.15 (Bluetooth), 802.16 (Broadband Wireless Access), 802.20 (Mobile Broadband Wireless Access)
  - 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

Wireless Network Types

□ Fixed networks

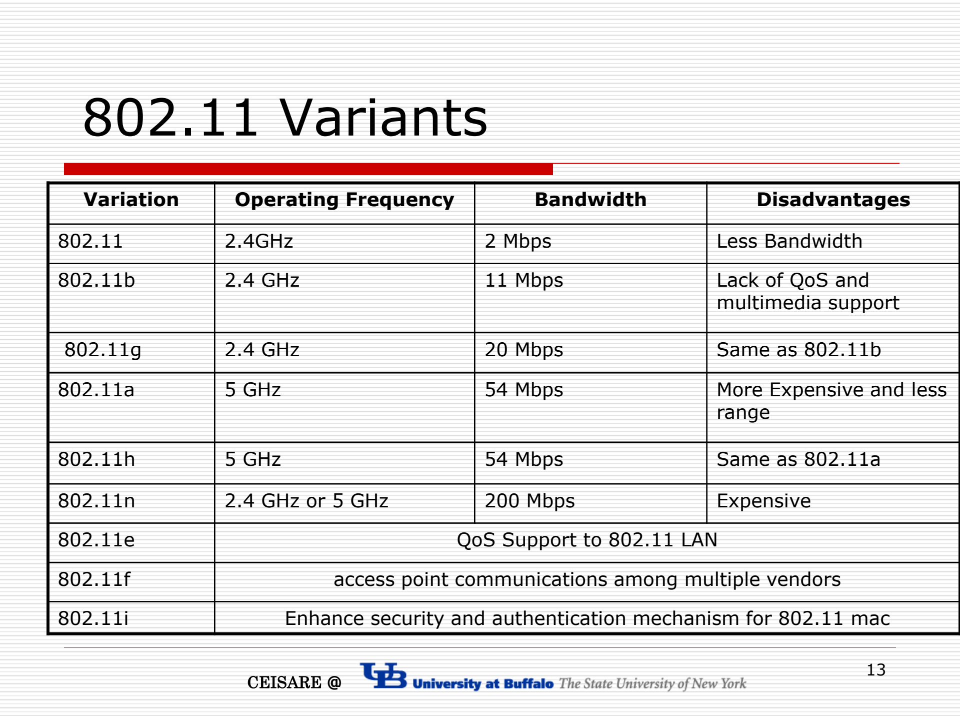
- Point-to-point network

□ Nomadic networks

- Point-to-multipoint network
- Computing devices are somewhat mobile
- 802.11b, 802.11g, 802.11a support this
- Becoming quite commonplace – coffee shop

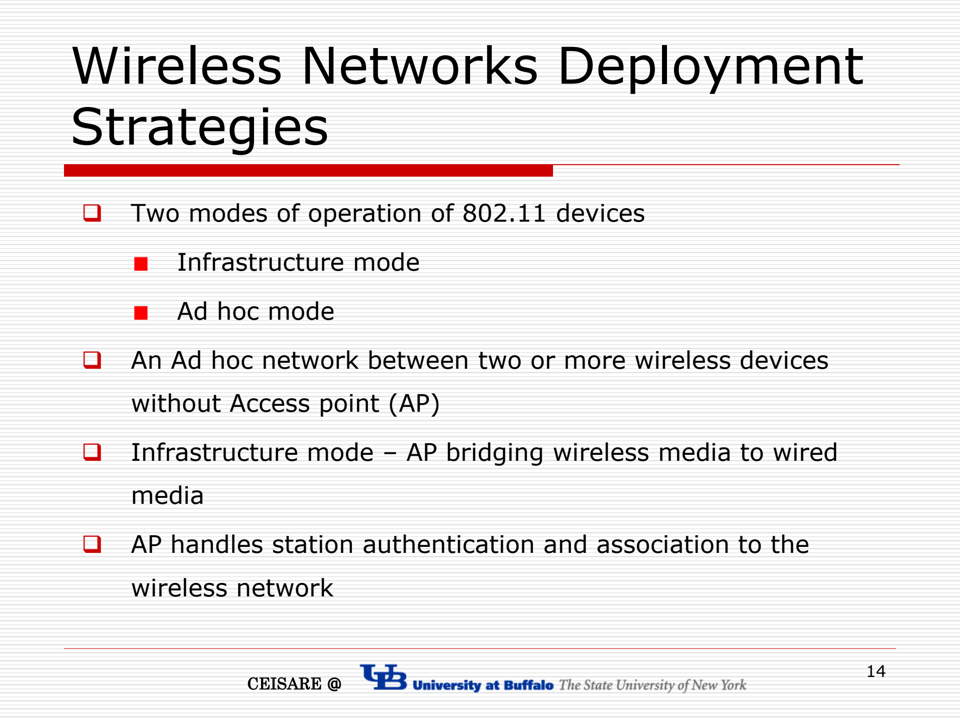
□ Mobile networks

- Must support high velocity mobility, 802.16e, 802.20 and CDMA 2000 standards



802.11 Variants

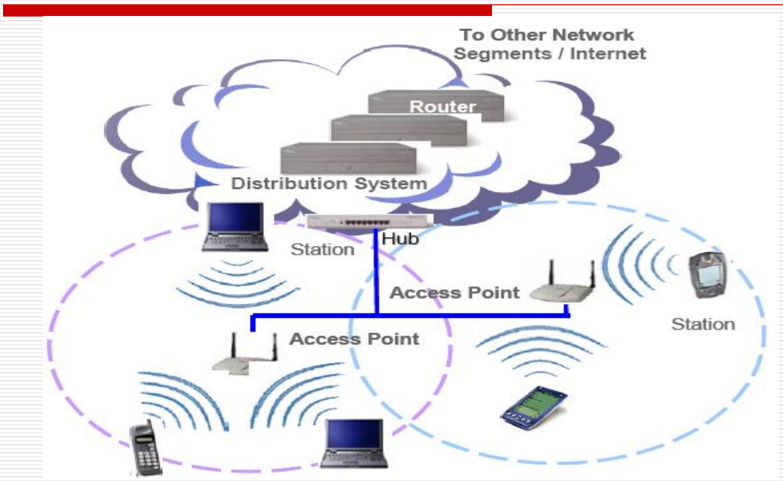
Variation	Operating Frequency	Bandwidth	Disadvantages
802.11	2.4GHz	2 Mbps	Less Bandwidth
802.11b	2.4 GHz	11 Mbps	Lack of QoS and multimedia support
802.11g	2.4 GHz	20 Mbps	Same as 802.11b
802.11a	5 GHz	54 Mbps	More Expensive and less range
802.11h	5 GHz	54 Mbps	Same as 802.11a
802.11n	2.4 GHz or 5 GHz	200 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		



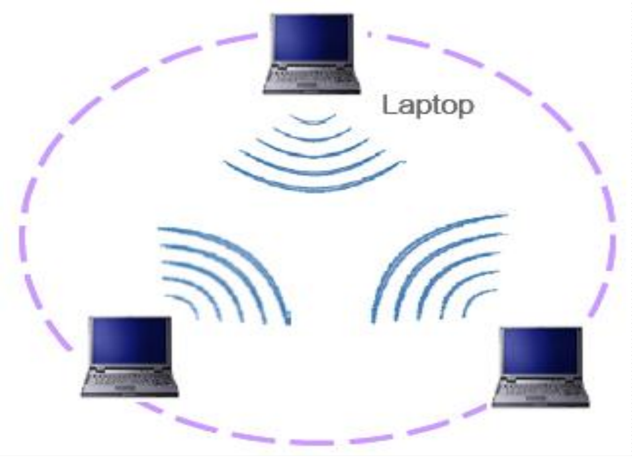
Wireless Networks Deployment Strategies

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

Infrastructure Mode Architecture



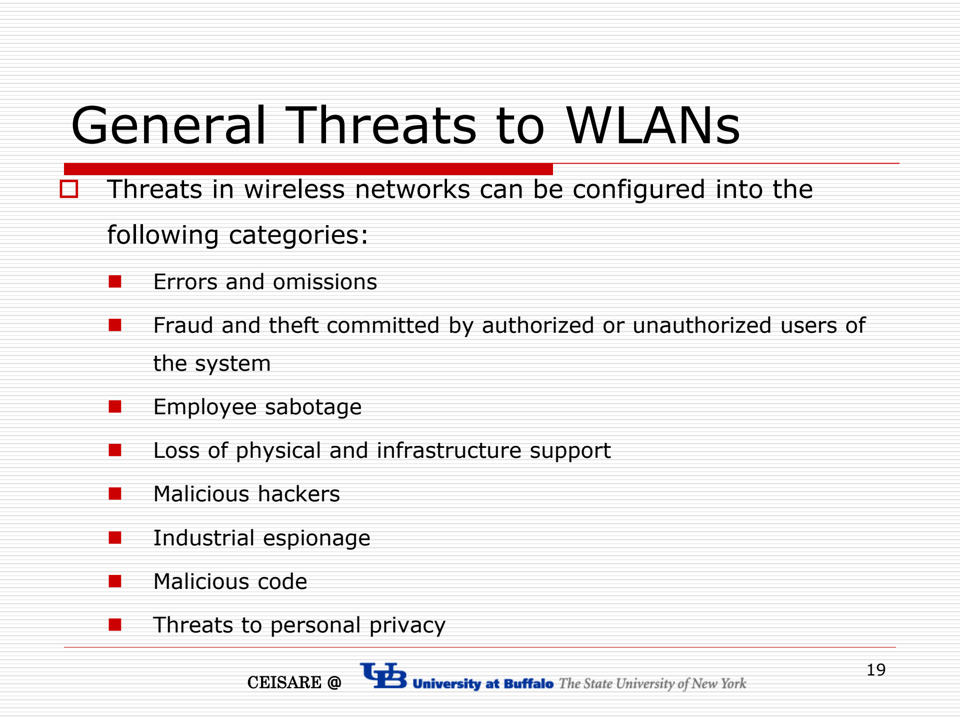
Ad-hoc Mode Architecture



DOONESBURY/ by Garry Trudeau
EXCUSE ME? YOU IN THERE!
RAP! RAP!
WHAT?
YOU'RE FREELOADING OFF MY HOME WIRELESS NETWORK, AREN'T YOU?
SO WHAT? I'M ON THE STREET. IT'S A FREE COUNTRY.
YEAH, BUT HIGH-SPEED ACCESS ISN'T! I'M PAYING FOR IT!
I SUPPOSE YOU ALSO PAY FOR MUSIC, MOVIES AND GAMES, TOO.
AS A MATTER OF FACT, I DO!
EXCELLENT. DON'T EVER CHANGE, MAN...
WITHOUT SOLID CITIZENS LIKE YOU, THERE WOULDN'T EVEN BE ANY COOL GOODS AND SERVICES FOR THE REST OF US! MY HAT'S OFF TO YOU, MAN!
OH...UH... THANKS...
NO PROBLEM. LISTEN, YOU MIGHT WANT TO CHECK OUT YOUR DAUGHTER'S E-MAIL.
7-21
UNIVERSAL PRESS SYNDICATE © 2002 G.B. Trudeau
www.doonesbury.com
GB Trudeau

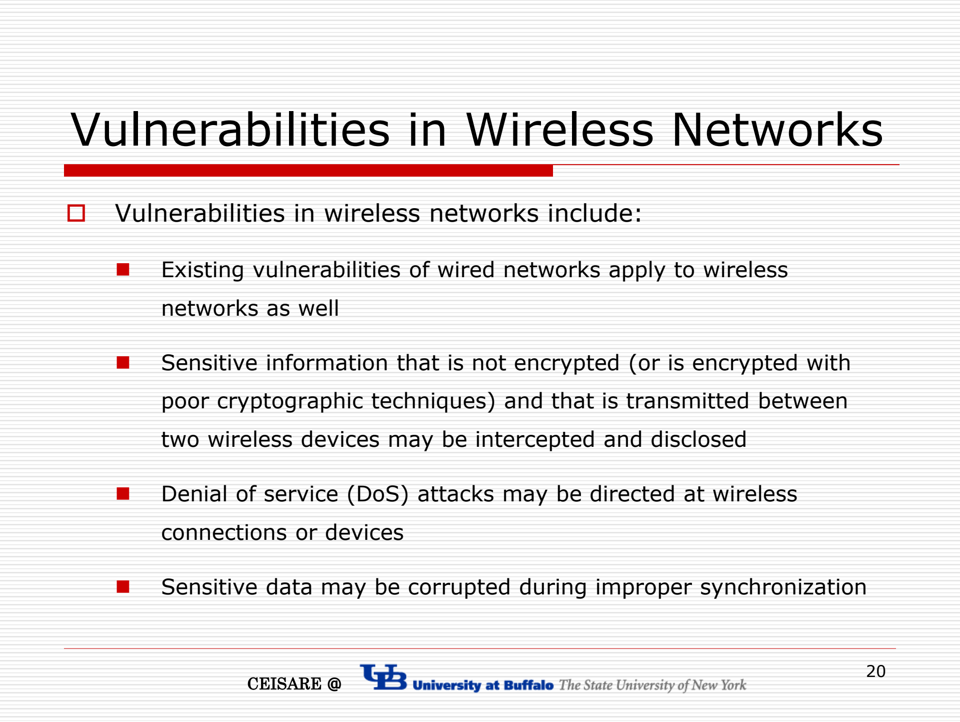
Wireless Security Challenges

- What are the major challenges?



General Threats to WLANs

- Threats in wireless networks can be configured into the following categories:
  - Errors and omissions
  - Fraud and theft committed by authorized or unauthorized users of the system
  - Employee sabotage
  - Loss of physical and infrastructure support
  - Malicious hackers
  - Industrial espionage
  - Malicious code
  - Threats to personal privacy



Vulnerabilities in Wireless Networks

- Vulnerabilities in wireless networks include:
  - Existing vulnerabilities of wired networks apply to wireless networks as well
  - Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed
  - Denial of service (DoS) attacks may be directed at wireless connections or devices
  - Sensitive data may be corrupted during improper synchronization

Vulnerabilities, Contd..

- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements
- Handheld devices are easily stolen and can reveal sensitive information
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations

Wi-Fi Evil Twins

- Evil twins are a significant menace to threaten the security of Internet users
- Anyone with suitable equipment can locate a hotspot and take its place, substituting their own “evil twin”
- There are no good solutions against it
- Strong authentication and encryption could be good defenses

WLAN - Security Problems

Attacks in WLANs can be classified as:

- Passive Attacks

  An attack in which an unauthorized party simply gains access to an asset and does not modify its content

  - Eavesdropping
  - Traffic Analysis

- Active Attacks

  An attack whereby an unauthorized party makes modifications to a message, data stream, or file

  - Masquerading
  - Replay
  - Message Modification
  - Denial of Service (DoS)

WLAN Security Goals

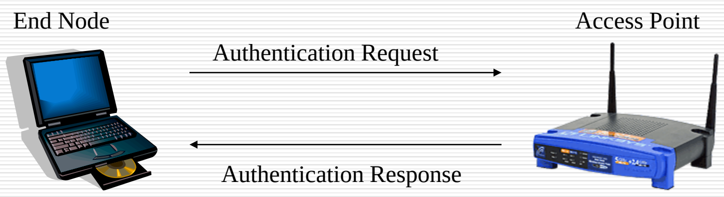
- There are four goals one should aim for when installing a wireless network
  - **Access control** - Only authorized users should be allowed to use the wireless network
  - **Data integrity** - The network traffic should be secure against tampering
  - **Confidentiality** - The user should be protected against a third party listening to the conversation
  - **Availability of service** - The service should be secured against Denial of Service (DoS) attacks

Basic WLAN Security Mechanisms

- Security Problems - 802.11 family faces the same problems
  - Sniffing and War driving
- Following security mechanisms exist
  - Service Set Identifier (SSID)
  - MAC Address filtering
  - Open System Authentication
  - Shared Key Authentication
  - Wired Equivalent Privacy (WEP) protocol
- 802.11 products are shipped by the vendors with all security mechanisms disabled !!
  - Allows any wireless node (NIC) to access the network
  - Walk around and gain access to the network

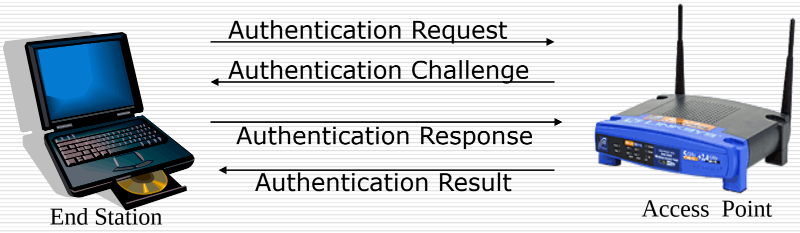
Open System Authentication

- The default authentication protocol for 802.11
- Authenticates anyone who requests authentication (null authentication)



Shared Key Authentication

- □ This assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network
- □ Stations authenticate through shared knowledge of the secret key
- □ Use of shared key authentication requires implementation of the 'Wired Equivalent Privacy' algorithm



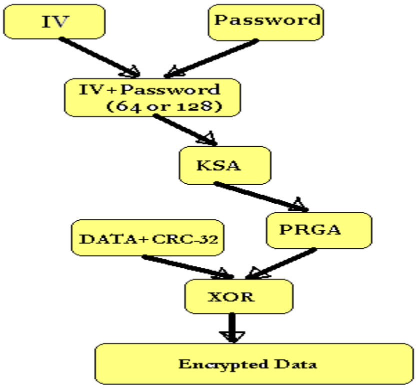
Wired Equivalence Privacy (WEP)

- □ Designed to provide confidentiality to a wireless network similar to that of standard LANs
- □ WEP is essentially the RC4 symmetric key cryptographic algorithm (same key for encrypting and decrypting)
- □ Transmitting station concatenates 40 bit key with a 24 bit Initialization Vector (IV) to produce pseudorandom key stream
- □ Plaintext is XORed with the pseudorandom key stream to produce ciphertext

Wired Equivalence Privacy (WEP)

- □ Ciphertext is concatenated with IV and transmitted over the wireless medium
- □ Receiving station reads the IV, concatenates it with the secret key to produce local copy of the pseudorandom key stream
- □ Received ciphertext is XORed with the key stream generated to get back the plaintext

WEP Encryption Algorithm



IV

Password

IV+Password (64 or 128)

KSA

DATA+CRC-32

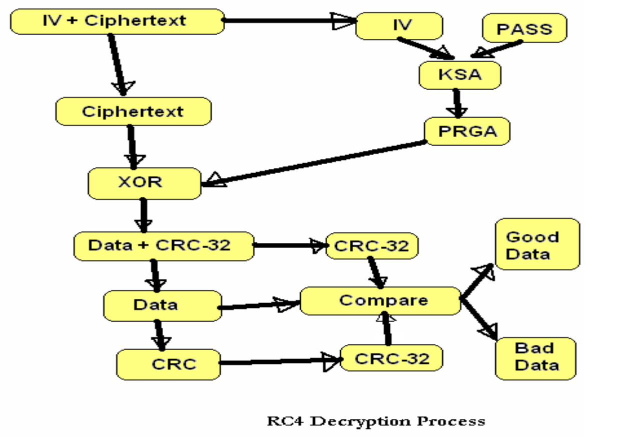
PRGA

XOR

Encrypted Data

RC4 Encryption Process

WEP Decrypting Algorithm



RC4 Decryption Process

WEP Problems

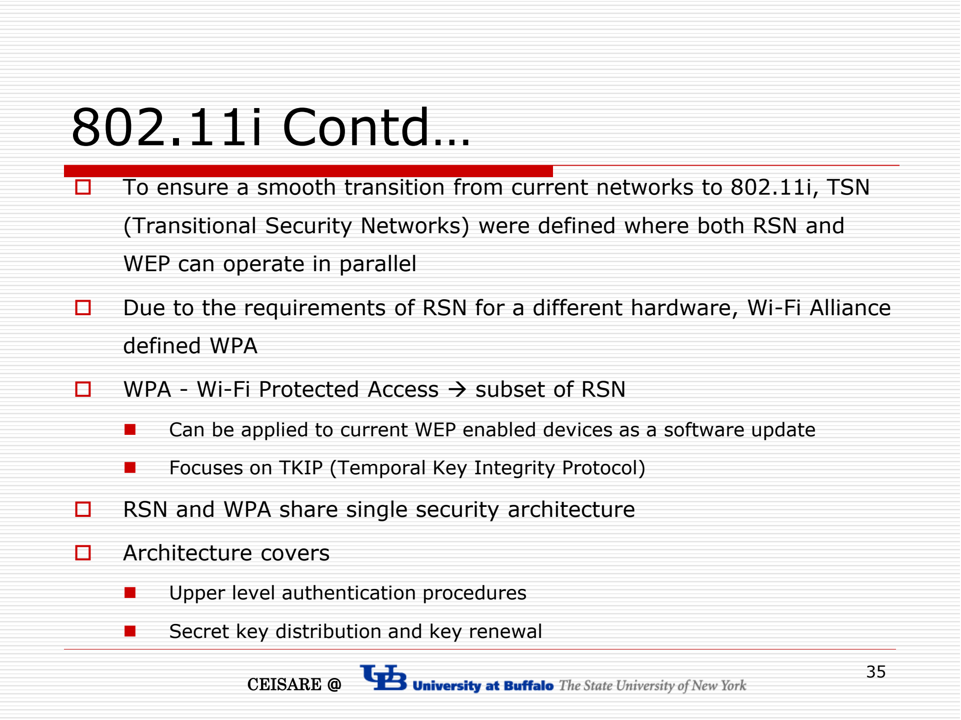
- □ There is no key management provision in the WEP protocol
- □ WEP has been broken! Walker (Oct 2000), Borisov et al. (Jan 2001), Fluhrer-Mantin -Shamir (Aug 2001)
- □ Unsafe at any key size: Testing reveals WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size
- □ More about this at:
- □ https://www.mattblaze.org/papers/others/rc4_ksaproc.pdf

802.11i Basics

- □ The wireless security standards

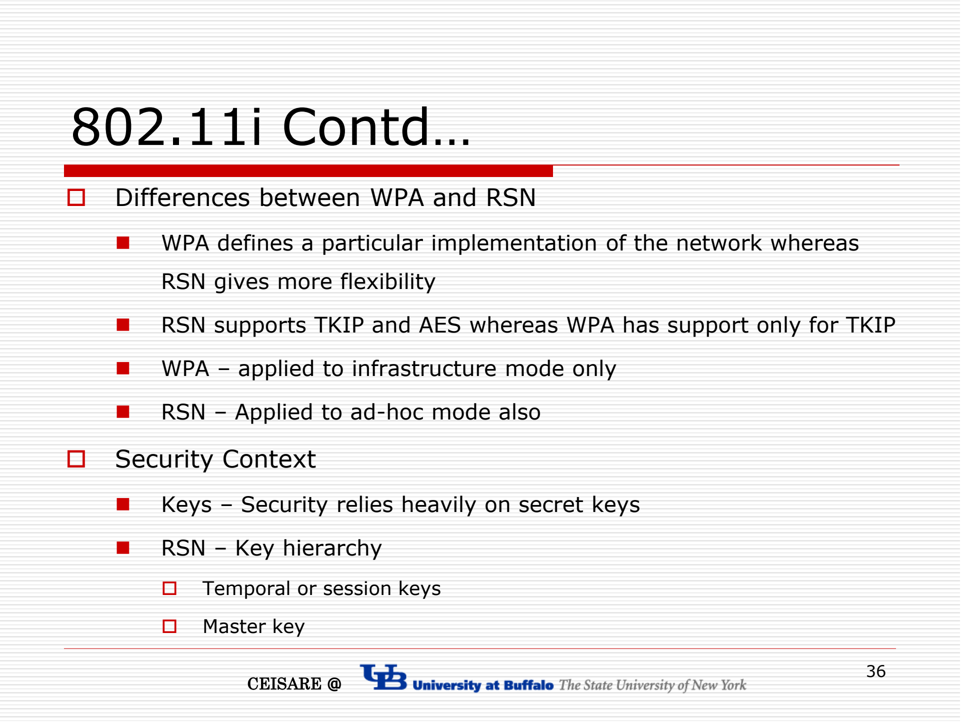
802.11i – The New Security Standard

- □ New generation of Security Standards
- □ Standard was ratified in June, 2004 and incorporated into 802.11-2007 standard
- □ Defines a security mechanism that operates between the Media Access Control (MAC) sublayer and the Network layer
- □ Introduced a new type of wireless network called RSN
- □ RSN - Robust Security Networks
  - ■ Based on AES (Advanced Encryption Standard) along with 802.1X and EAP (Extensible Authentication Protocol)
  - ■ Needs RSN compatible hardware to operate



802.11i Contd…

- □ To ensure a smooth transition from current networks to 802.11i, TSN (Transitional Security Networks) were defined where both RSN and WEP can operate in parallel
- □ Due to the requirements of RSN for a different hardware, Wi-Fi Alliance defined WPA
- □ WPA - Wi-Fi Protected Access → subset of RSN
  - ■ Can be applied to current WEP enabled devices as a software update
  - ■ Focuses on TKIP (Temporal Key Integrity Protocol)
- □ RSN and WPA share single security architecture
- □ Architecture covers
  - ■ Upper level authentication procedures
  - ■ Secret key distribution and key renewal



802.11i Contd…

- □ Differences between WPA and RSN
  - ■ WPA defines a particular implementation of the network whereas RSN gives more flexibility
  - ■ RSN supports TKIP and AES whereas WPA has support only for TKIP
  - ■ WPA – applied to infrastructure mode only
  - ■ RSN – Applied to ad-hoc mode also
- □ Security Context
  - ■ Keys – Security relies heavily on secret keys
  - ■ RSN – Key hierarchy
    - □ Temporal or session keys
    - □ Master key

802.11i Contd…

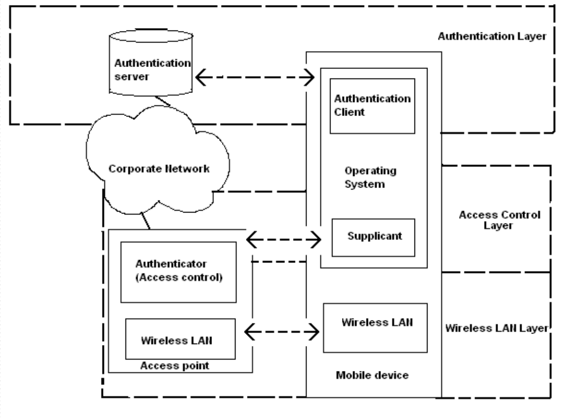
- Security Layers
  - *Wireless LAN layer*

    Raw communication, advertising capabilities, encryption, decryption
  - *Access control layer*

    Middle manager: manages the security context. Talks to the authentication layer to decide the establishment of security context and participates in generation of temporal keys
  - *Authentication layer*

    Layer where the policy decisions are made and proof of identity is accepted or rejected

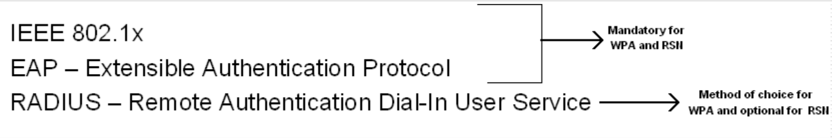
802.11i Contd…



Relationship of Layers

Access Control Methods

- Access Control Mechanism to separate authorized and unauthorized personnel
- Protocols used to implement Access Control in RSN and WPA are:
  - 802.1X
  - EAP
  - RADIUS



IEEE 802.1x

EAP – Extensible Authentication Protocol

RADIUS – Remote Authentication Dial-In User Service

Mandatory for WPA and RSN
Method of choice for WPA and optional for RSN

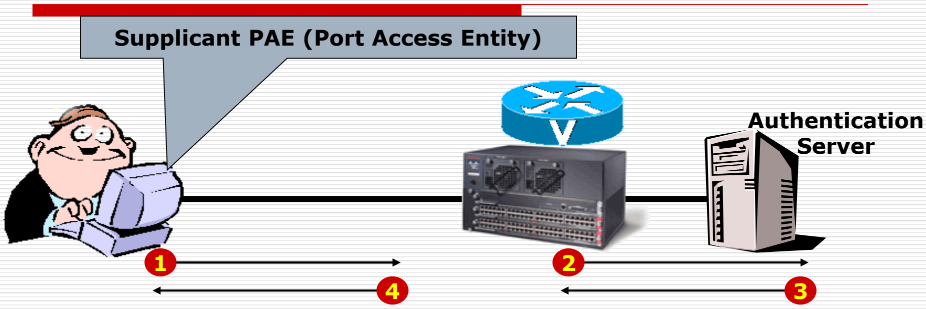
Access Control Methods

- Elements of Access Control:
  - Supplicant
  - Authenticator
  - Authorizer
- Steps in Access Control:
  - Authenticator is alerted by the supplicant
  - Supplicant identifies himself
  - Authenticator requests authorization from authorizer
  - Authorizer indicates Yes or No
  - Authenticator allows or blocks device

802.1X

- Divides the network into three entities:
  - Supplicant
  - Authenticator
  - Authentication Server
- Works between the supplicant (client) and the authenticator (network device)
- Medium independent (Wired, Wireless, Cable/Fiber)
- Uses EAP to support Multiple authentication methods like:
  - EAP-TLS (certificates)
  - PEAP/TTLS (password)

802.1X Components



1 User activates link (i.e., connects to the access point)

2 Switch requests authentication server if user is authorized to access LAN

3 Authentication server responds with authority access

4 Switch opens controlled port (if authorized) for user to access LAN

Role of RADIUS in WPA

- □ **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
- □ De-Facto Standard For Remote Authentication
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Handshake Authentication Protocol)
- □ Used for communication between APs and AS
- □ RADIUS facilitates centralized user administration required for many applications, e.g., ISPs
- □ Perhaps not used in home installations
- □ WPA mandates the use of RADIUS authentication
- □ Optional for RSNs – RSNs use Kerberos

Student Presentation Topics

- □ Secure Routing in Ad hoc Networks
- □ Key Management in Ad Hoc and Sensor Networks
- □ Attacks in Sensor Networks
- □ Trust Issues in Wireless Networks
- □ Mesh Networks Security
- □ Vehicular Networks Security
- □ Smart Grid Security
- □ Smartphone Security
- □ Internet of Things (IoT) Security