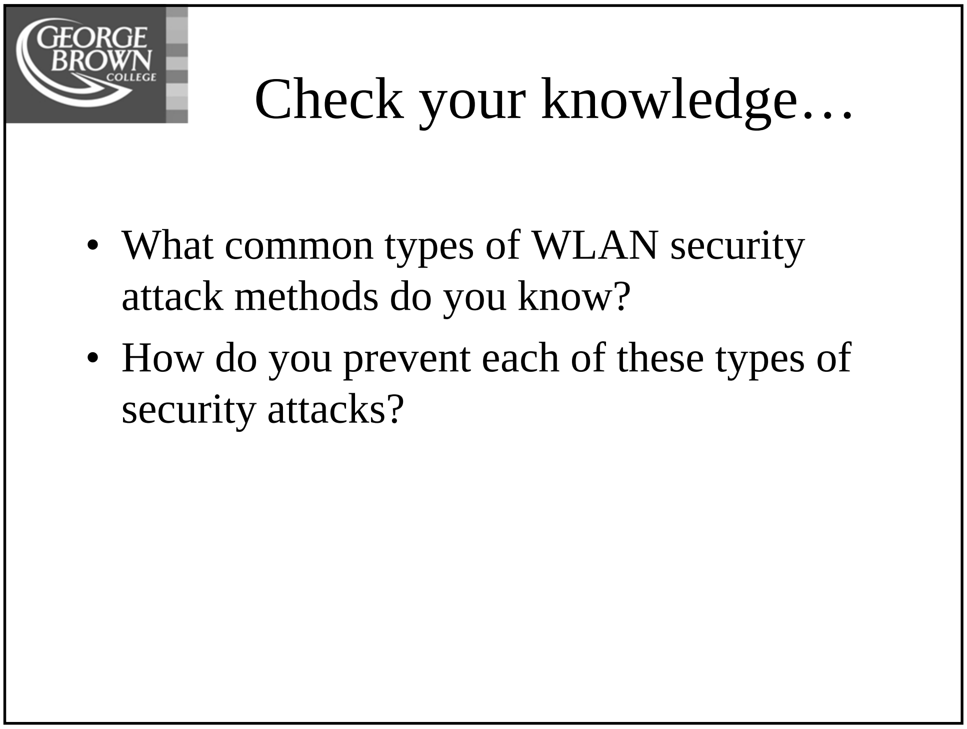
Wireless Security

Chapters 9 & 10

COMP3049 – CWNA

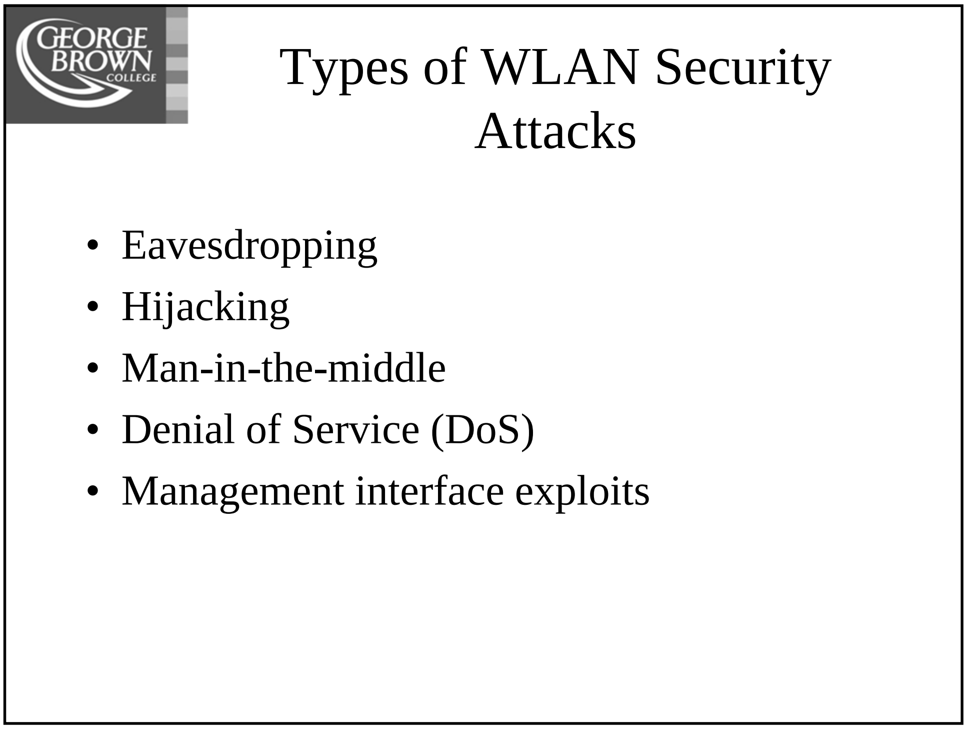
Objectives

- Describe the different types of security attacks
- Outline how to identify WLAN security attacks
- Explain how to prevent WLAN security attacks
- Identify the strengths, weaknesses appropriate uses and implementation of IEEE 802.11 security-related items
- Illustrate the various client-related wireless security solutions
- Show the appropriate applications of WLAN security and management features



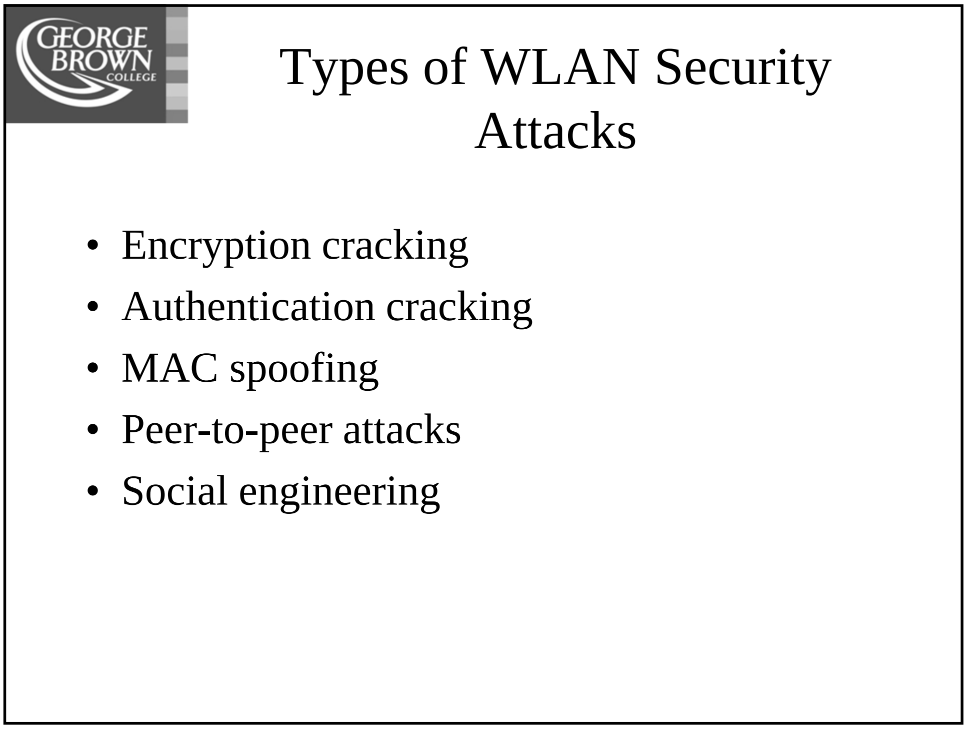
Check your knowledge…

- What common types of WLAN security attack methods do you know?
- How do you prevent each of these types of security attacks?



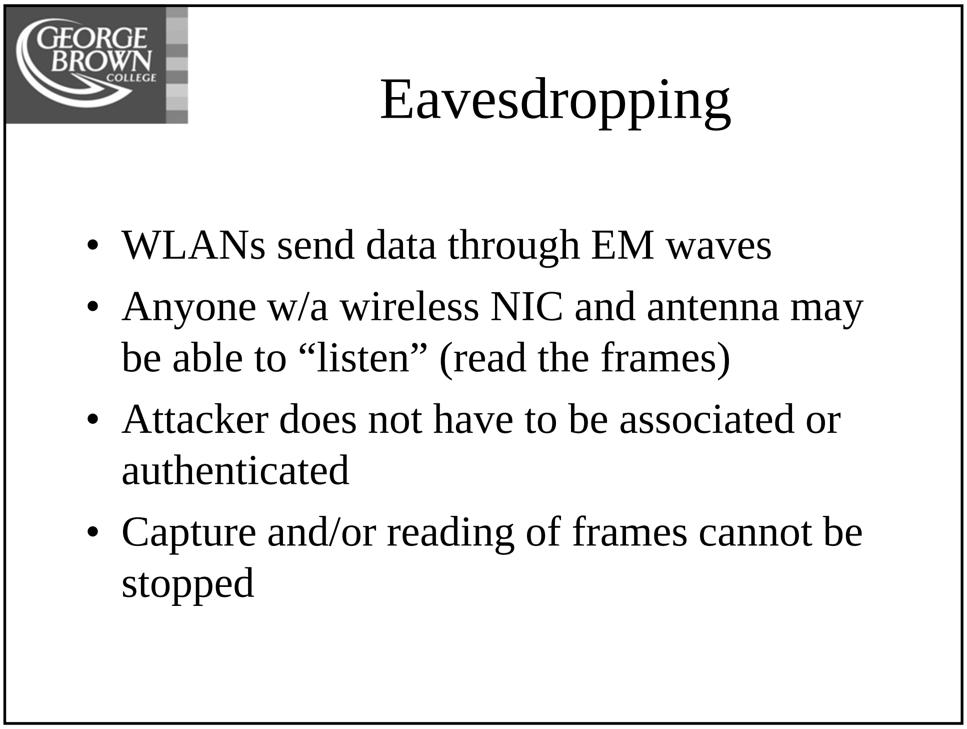
Types of WLAN Security Attacks

- Eavesdropping
- Hijacking
- Man-in-the-middle
- Denial of Service (DoS)
- Management interface exploits



Types of WLAN Security Attacks

- Encryption cracking
- Authentication cracking
- MAC spoofing
- Peer-to-peer attacks
- Social engineering



Eavesdropping

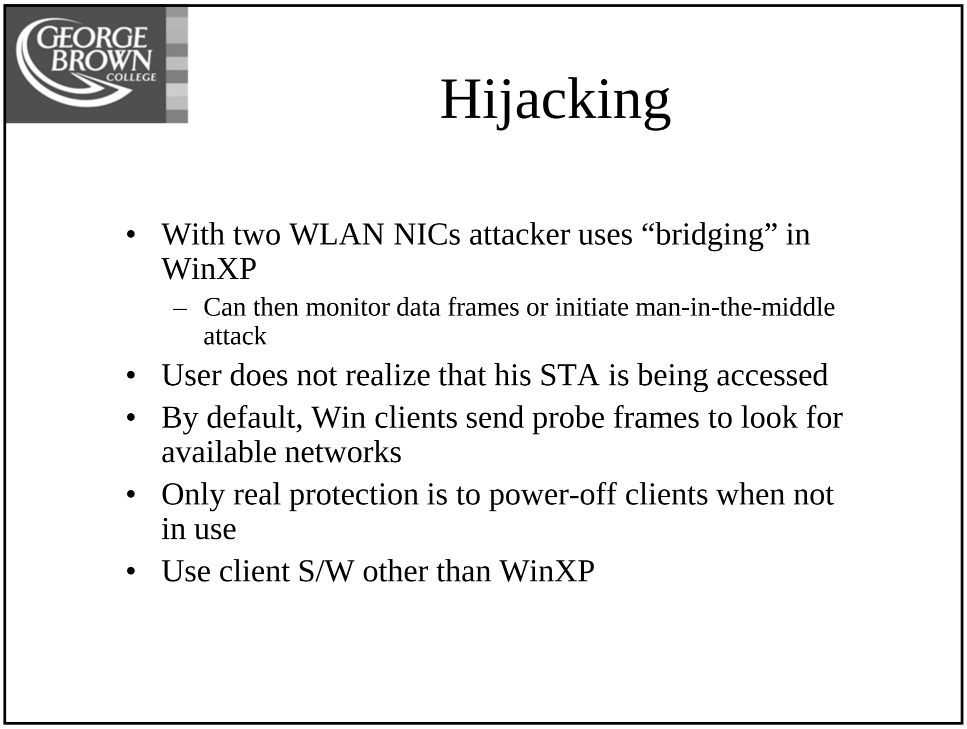
- WLANs send data through EM waves
- Anyone w/a wireless NIC and antenna may be able to “listen” (read the frames)
- Attacker does not have to be associated or authenticated
- Capture and/or reading of frames cannot be stopped

Eavesdropping

- Public Hotspots and corporate data
- Both commercial and freeware applications can be used for this purpose
- Pre-cursor to other types of attack

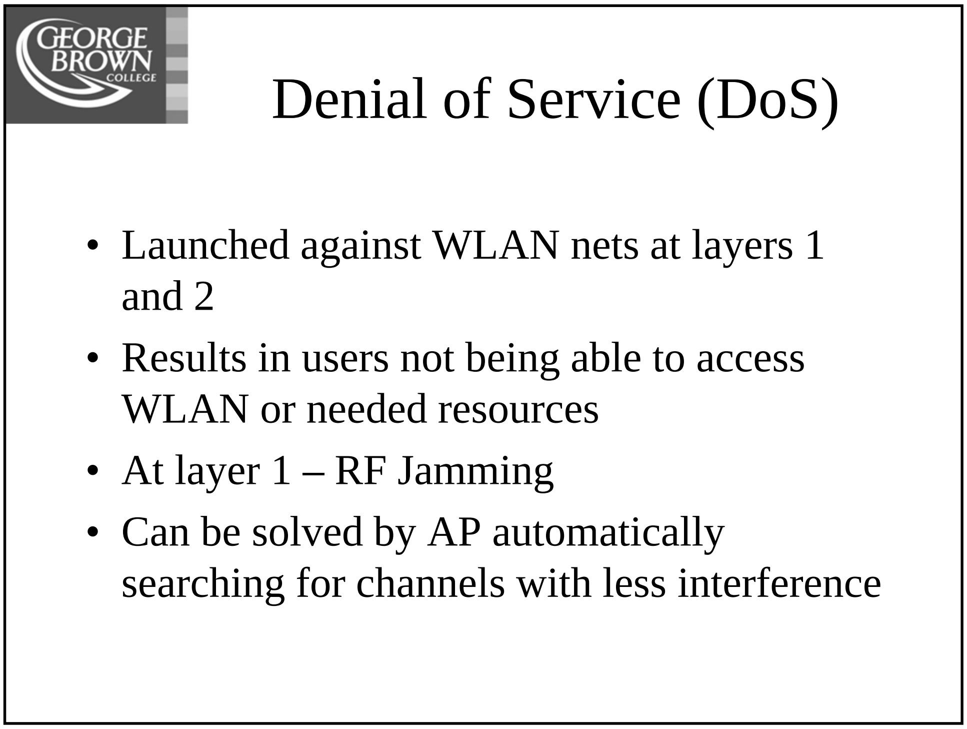
Hijacking

- Unauthorized user takes control of another’s WLAN connection
- Done at layer 2 for DoS and layer 3 for other attacks
  - Attacker uses AP software on laptop
  - Configures AP S/W to use same SSID
  - Sends a de-authentication frame or generates interference, forcing re-association
  - Since attacker’s AP is closer and has stronger signal, user device associates with attacker’s device



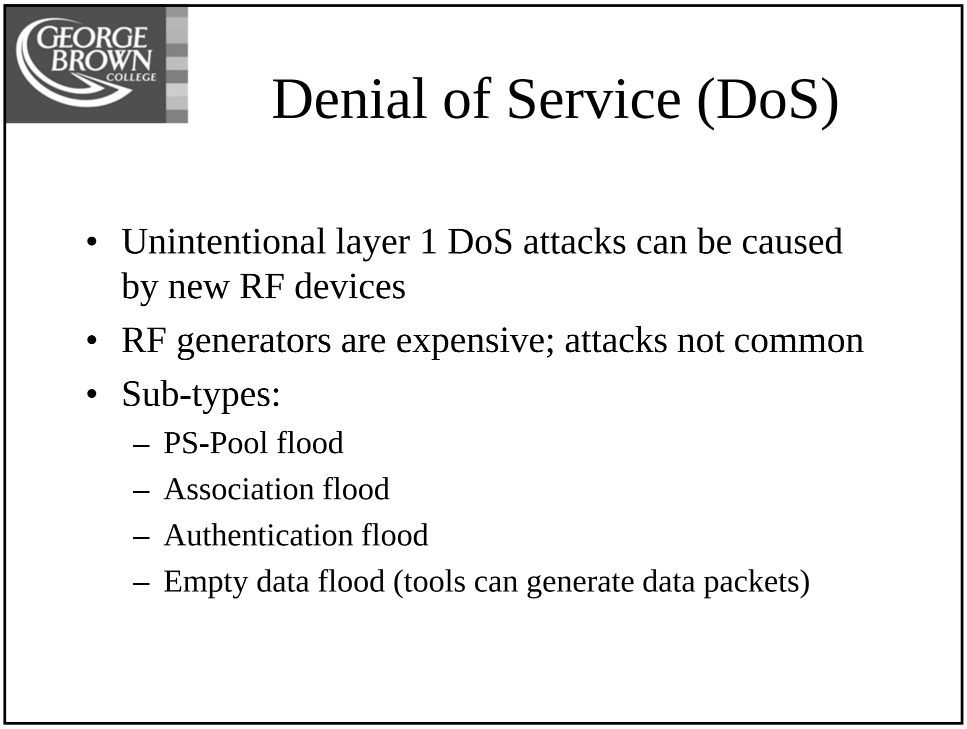
Hijacking

- With two WLAN NICs attacker uses “bridging” in WinXP
  - Can then monitor data frames or initiate man-in-the-middle attack
- User does not realize that his STA is being accessed
- By default, Win clients send probe frames to look for available networks
- Only real protection is to power-off clients when not in use
- Use client S/W other than WinXP



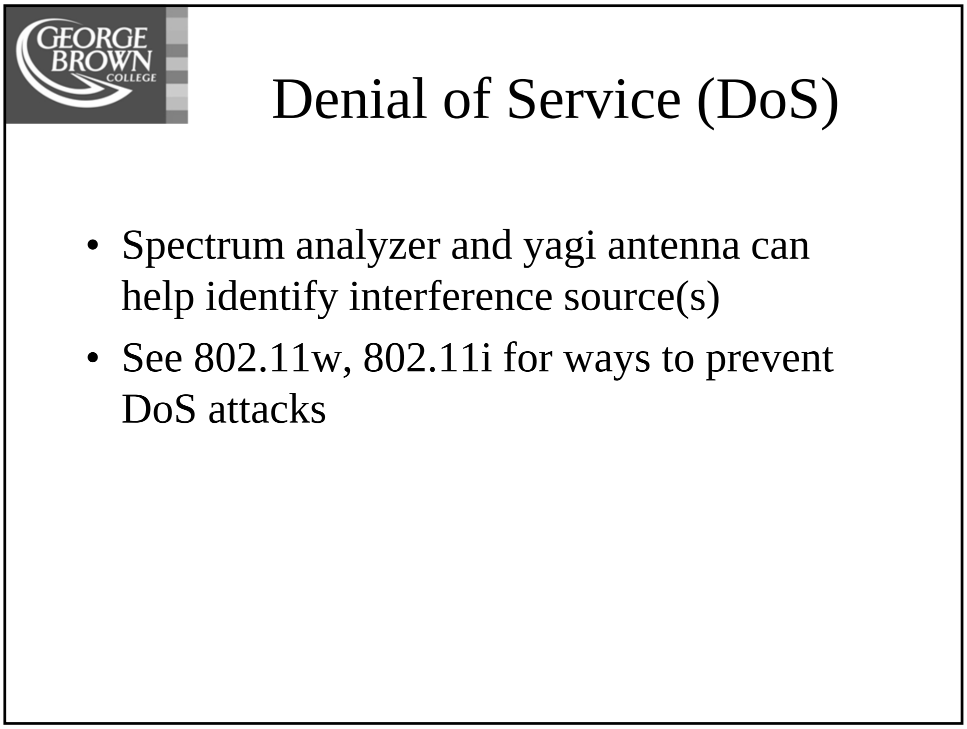
Denial of Service (DoS)

- Launched against WLAN nets at layers 1 and 2
- Results in users not being able to access WLAN or needed resources
- At layer 1 – RF Jamming
- Can be solved by AP automatically searching for channels with less interference



Denial of Service (DoS)

- Unintentional layer 1 DoS attacks can be caused by new RF devices
- RF generators are expensive; attacks not common
- Sub-types:
  - PS-Pool flood
  - Association flood
  - Authentication flood
  - Empty data flood (tools can generate data packets)



Denial of Service (DoS)

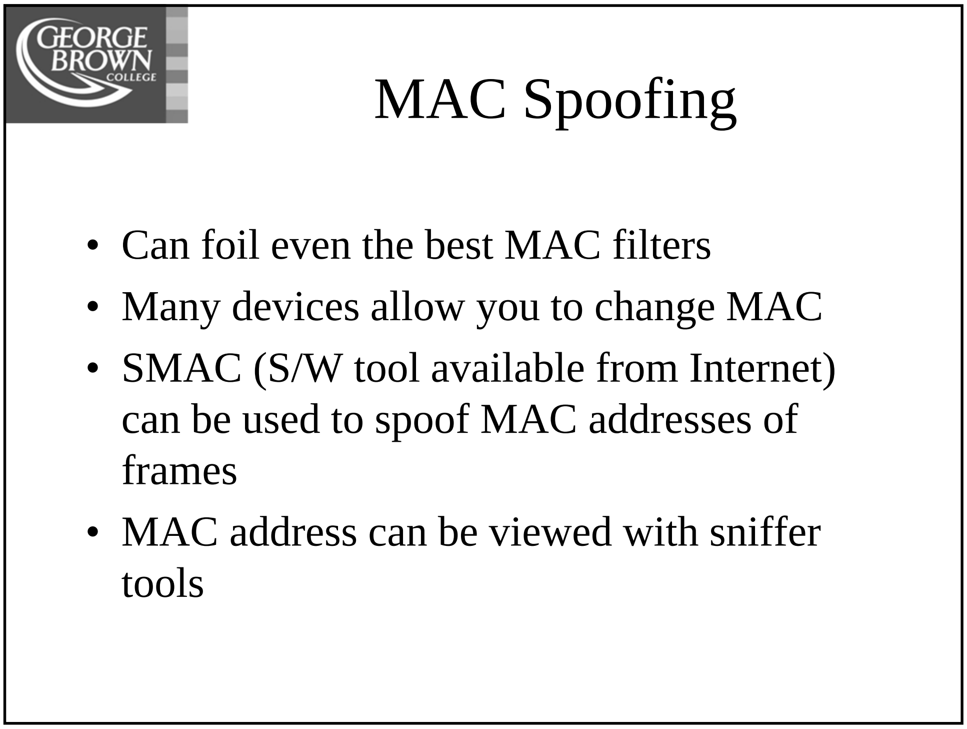
- Spectrum analyzer and yagi antenna can help identify interference source(s)
- See 802.11w, 802.11i for ways to prevent DoS attacks

Management Interface Exploits

- Attacker uses IP address and attempts to connect to AP:
  - Using browser
  - Using SNMP application
  - Using Telnet
- APs should use:
  - SSH instead of Telnet
  - HTTPS (SSL/TLS) for secure encrypted management using a browser

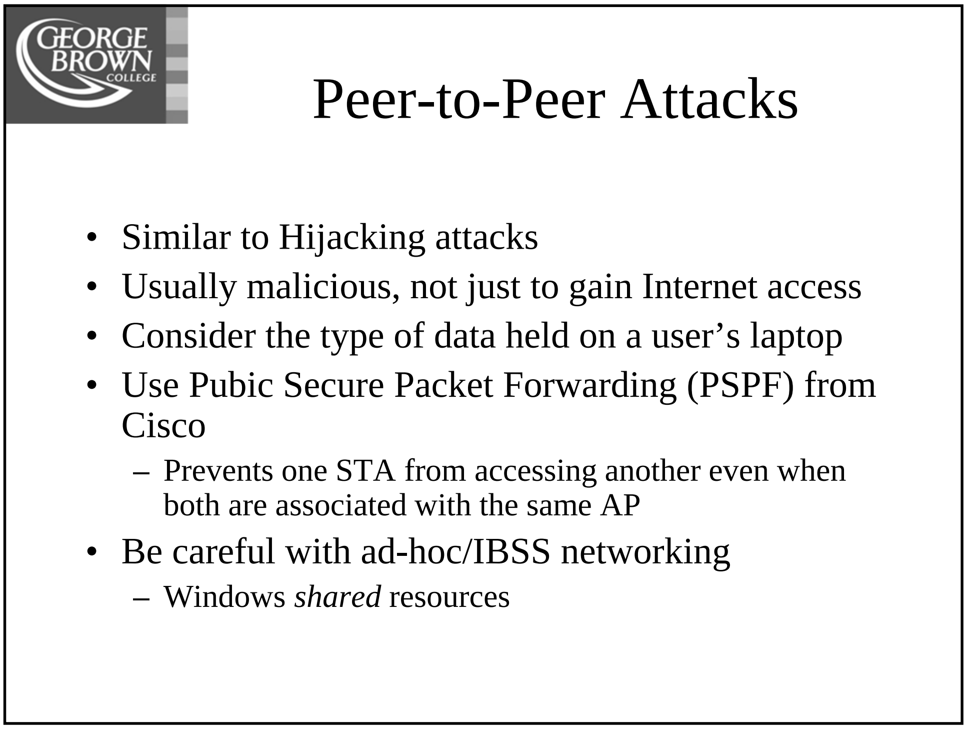
Encryption & Authentication/ Cracking

- WEP keys can be decrypted in about 3 to 6 minutes when the WLAN is busy
- Even Cisco LEAP has weaknesses
- If attacker captures four-way handshake for authentication, even WPA-PSK can be cracked (coWPAtty)
- Avoid dictionary words
- Use 802.11i/802.1X, PEAP, RADIUS instead



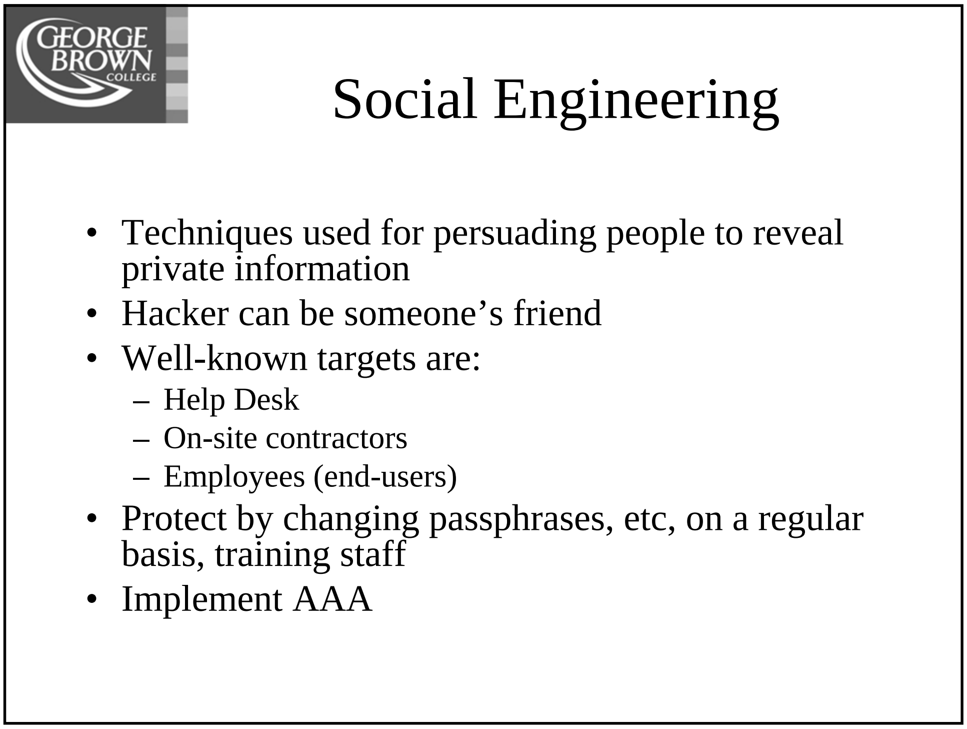
MAC Spoofing

- Can foil even the best MAC filters
- Many devices allow you to change MAC
- SMAC (S/W tool available from Internet) can be used to spoof MAC addresses of frames
- MAC address can be viewed with sniffer tools



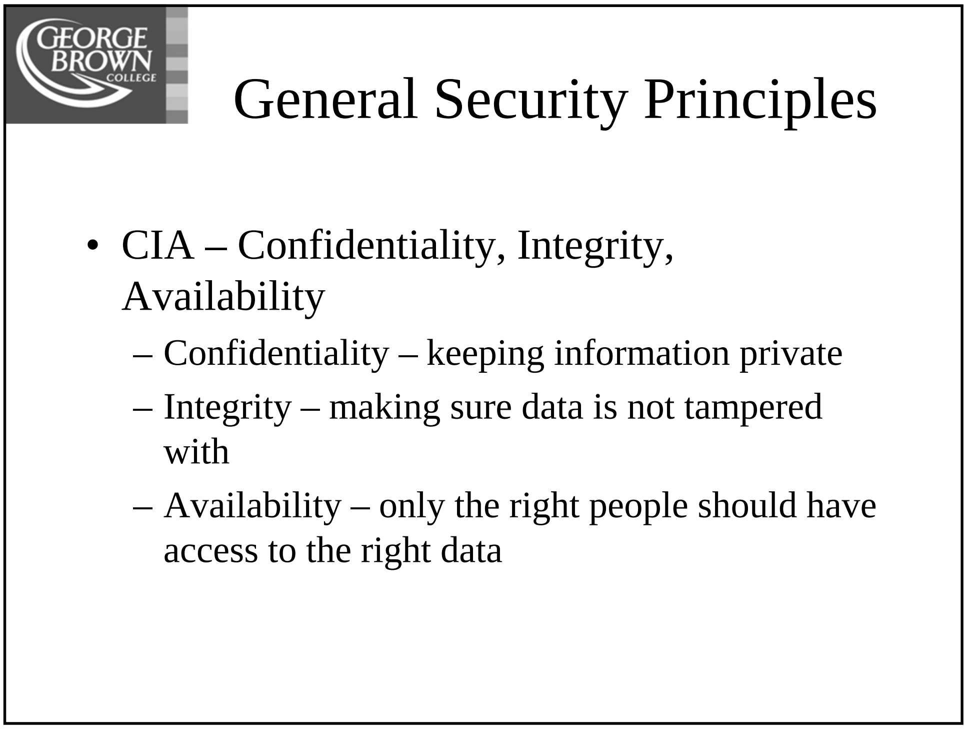
Peer-to-Peer Attacks

- Similar to Hijacking attacks
- Usually malicious, not just to gain Internet access
- Consider the type of data held on a user’s laptop
- Use Pubic Secure Packet Forwarding (PSPF) from Cisco
  - Prevents one STA from accessing another even when both are associated with the same AP
- Be careful with ad-hoc/IBSS networking
  - Windows *shared* resources



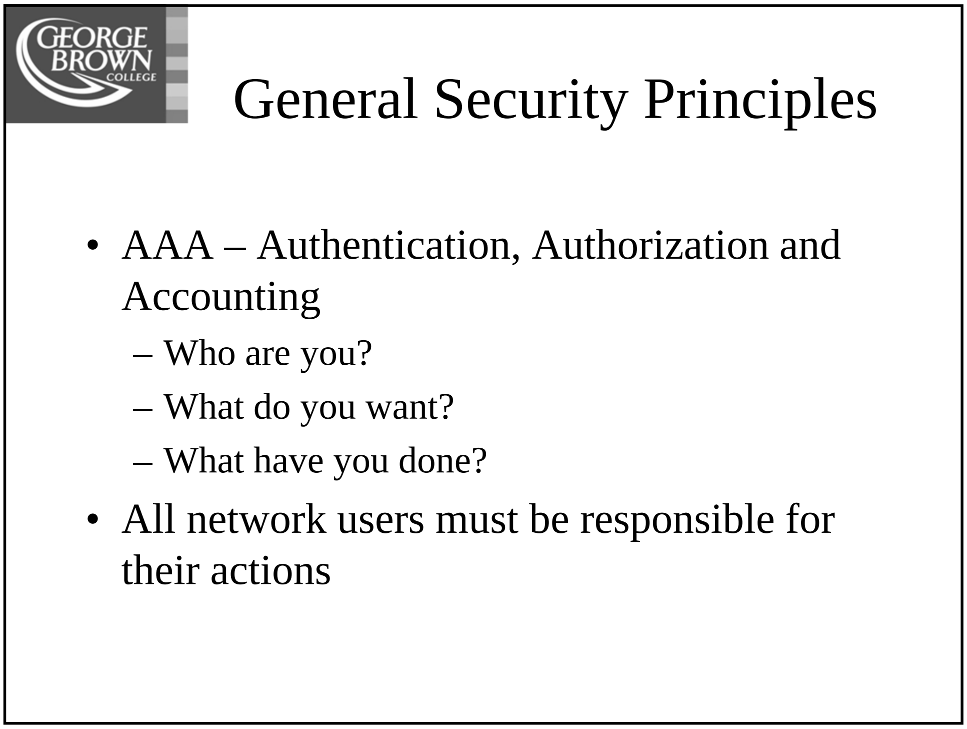
Social Engineering

- Techniques used for persuading people to reveal private information
- Hacker can be someone's friend
- Well-known targets are:
  - Help Desk
  - On-site contractors
  - Employees (end-users)
- Protect by changing passphrases, etc, on a regular basis, training staff
- Implement AAA



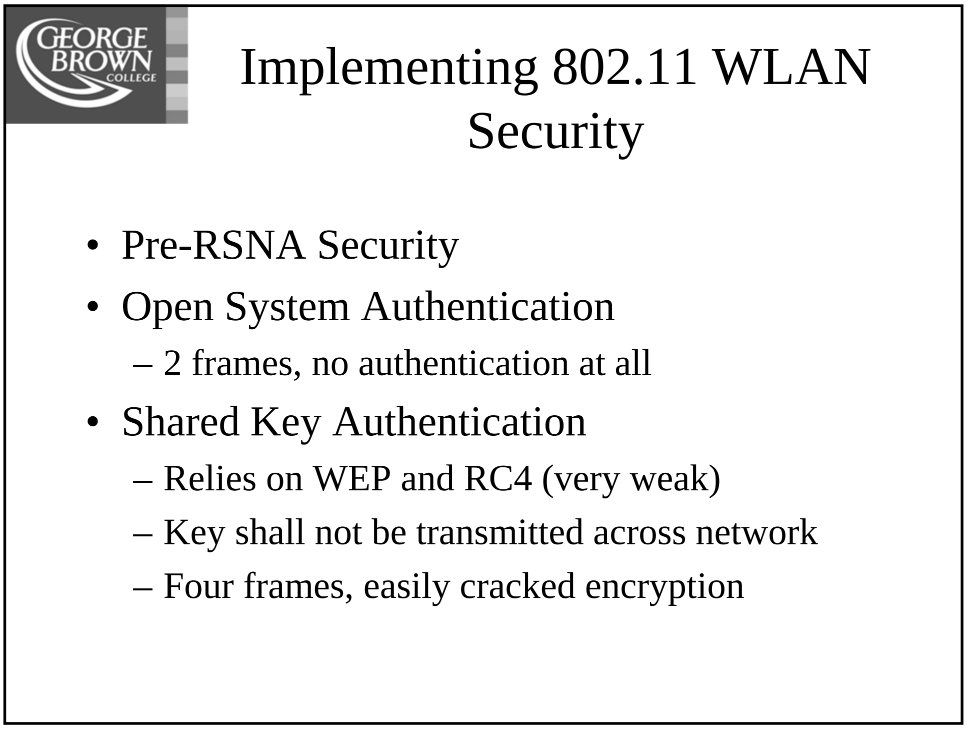
General Security Principles

- CIA – Confidentiality, Integrity, Availability
  - Confidentiality – keeping information private
  - Integrity – making sure data is not tampered with
  - Availability – only the right people should have access to the right data



General Security Principles

- AAA – Authentication, Authorization and Accounting
  - Who are you?
  - What do you want?
  - What have you done?
- All network users must be responsible for their actions



Implementing 802.11 WLAN Security

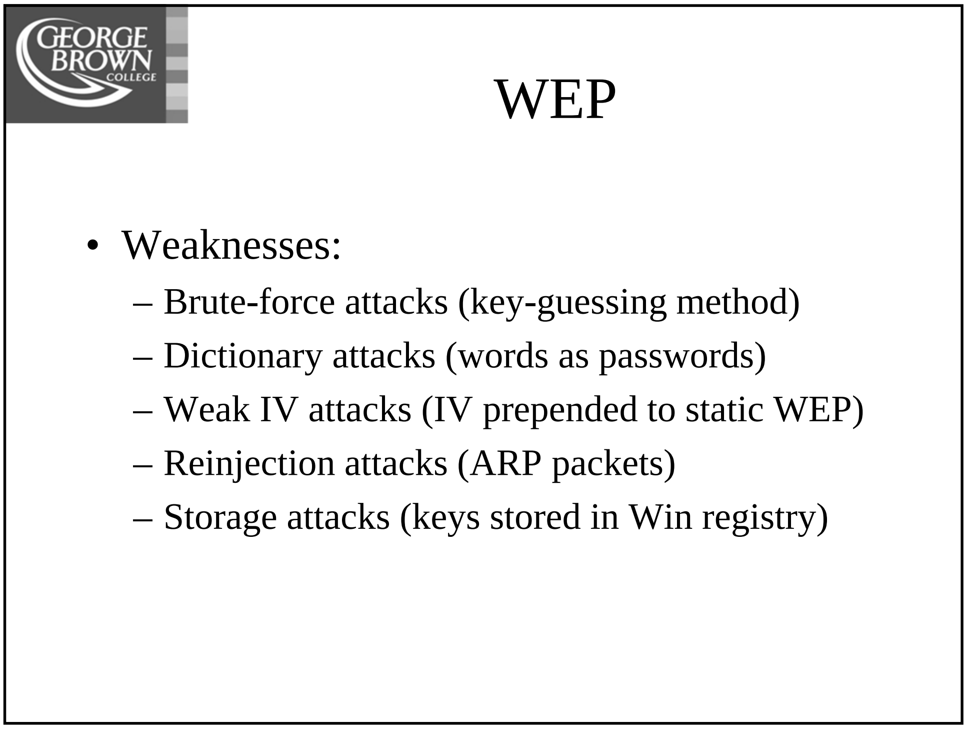
- Pre-RSNA Security
- Open System Authentication
  - 2 frames, no authentication at all
- Shared Key Authentication
  - Relies on WEP and RC4 (very weak)
  - Key shall not be transmitted across network
  - Four frames, easily cracked encryption

Wired Equivalent Privacy - WEP

- WEP uses either 40-bit or 104-bit plus RC4 algorithm for encryption
- 64-bit and 128-bit encryption (less 24-bit IV)
- IV is non-static 24-bit number used for each frame
- Only 16,277,216 possible unique IVs

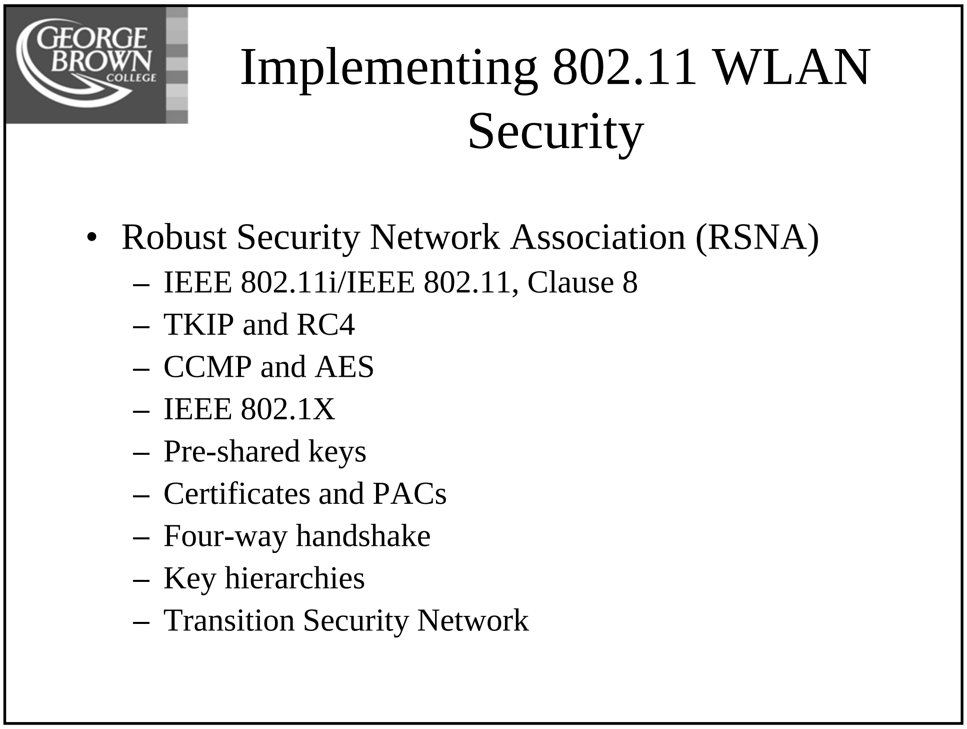
WEP

- Some vendors implemented non-standard encryption (152-bit = 128 + 24)
  - This requires same vendor equipment (specialized *supplicant*)
- Only protects data payload
  - Headers not encrypted
- Layer 2 security implementation



WEP

- Weaknesses:
  - – Brute-force attacks (key-guessing method)
  - – Dictionary attacks (words as passwords)
  - – Weak IV attacks (IV prepended to static WEP)
  - – Reinjection attacks (ARP packets)
  - – Storage attacks (keys stored in Win registry)



Implementing 802.11 WLAN Security

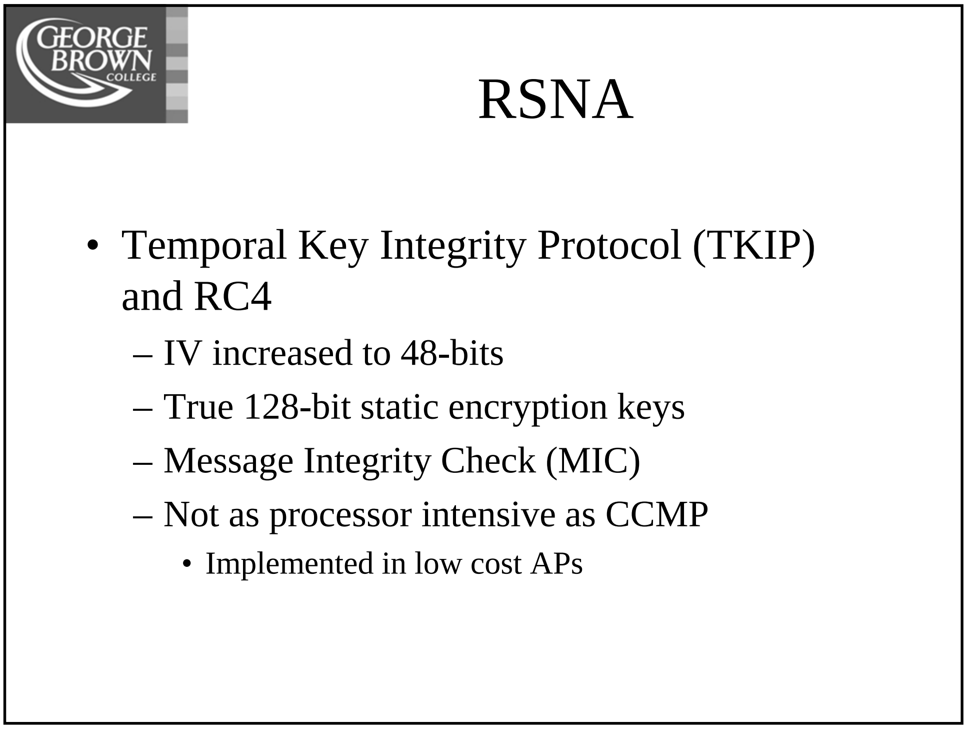
- Robust Security Network Association (RSNA)
  - – IEEE 802.11i/IEEE 802.11, Clause 8
  - – TKIP and RC4
  - – CCMP and AES
  - – IEEE 802.1X
  - – Pre-shared keys
  - – Certificates and PACs
  - – Four-way handshake
  - – Key hierarchies
  - – Transition Security Network

RSNA

- IEEE 802.11, Clause 8 ratified in 2004
- Allows security for WLANs to evolve
- Can only truly be established if mutual authentication occurs (AP/client)
- RSN – Robust Security Network
  - Four-way handshake
  - Beacon indicates that WEP is not used

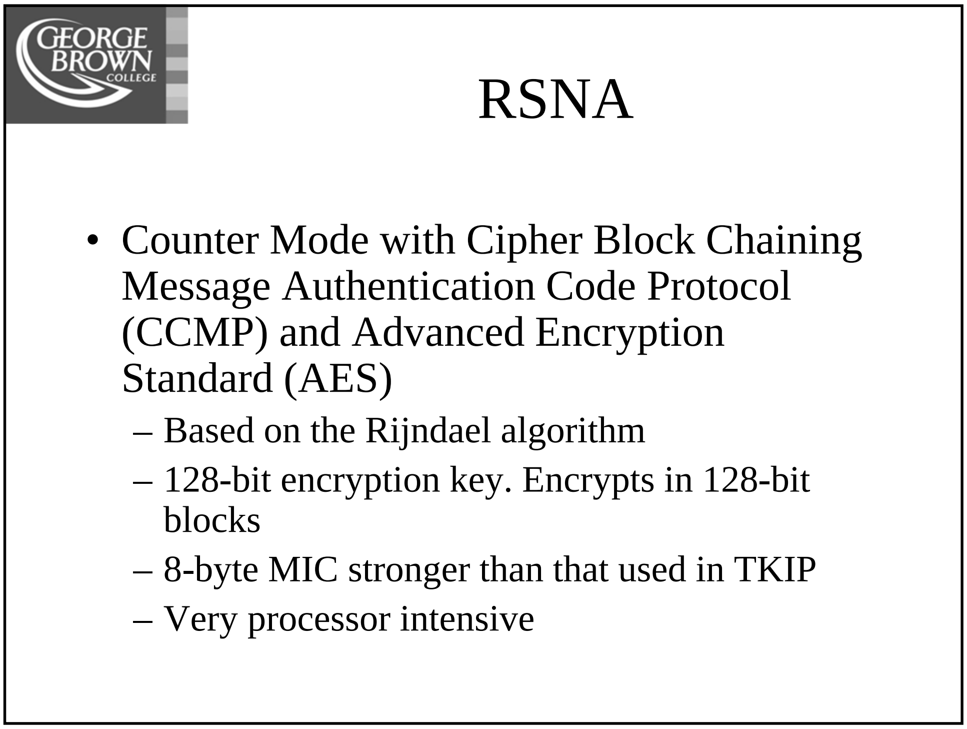
RSNA

- Four-way Handshake
  - Pairwise key management protocol
  - Confirms mutual possession of a pairwise master key (PMK)
- Pairwise Master Key (PMK)
  - A key derived from EAP or obtained directly from a pre-shared key
- Group Temporal Key (GTK)
  - Key used to protect multicast and broadcast traffic



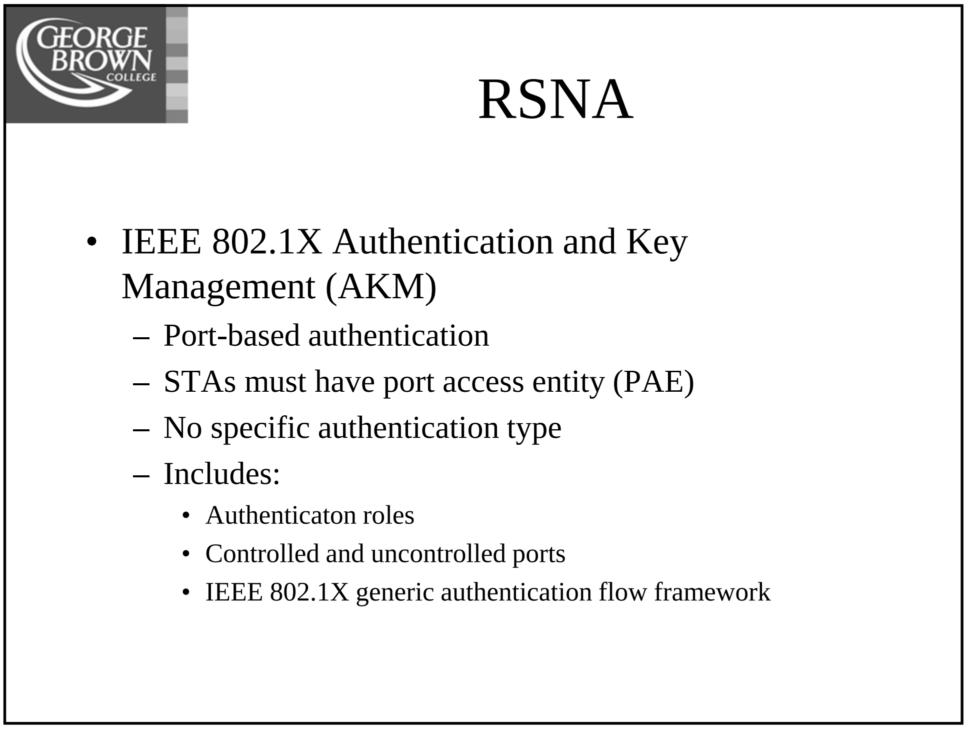
RSNA

- Temporal Key Integrity Protocol (TKIP) and RC4
  - – IV increased to 48-bits
  - – True 128-bit static encryption keys
  - – Message Integrity Check (MIC)
  - – Not as processor intensive as CCMP
    - Implemented in low cost APs



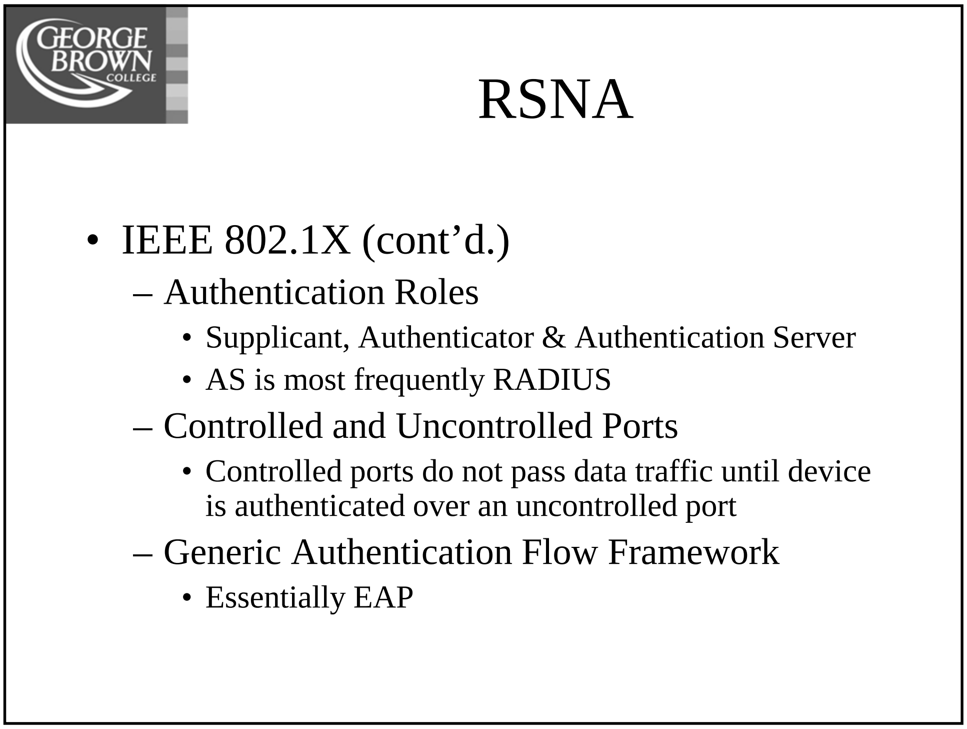
RSNA

- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES)
  - – Based on the Rijndael algorithm
  - – 128-bit encryption key. Encrypts in 128-bit blocks
  - – 8-byte MIC stronger than that used in TKIP
  - – Very processor intensive



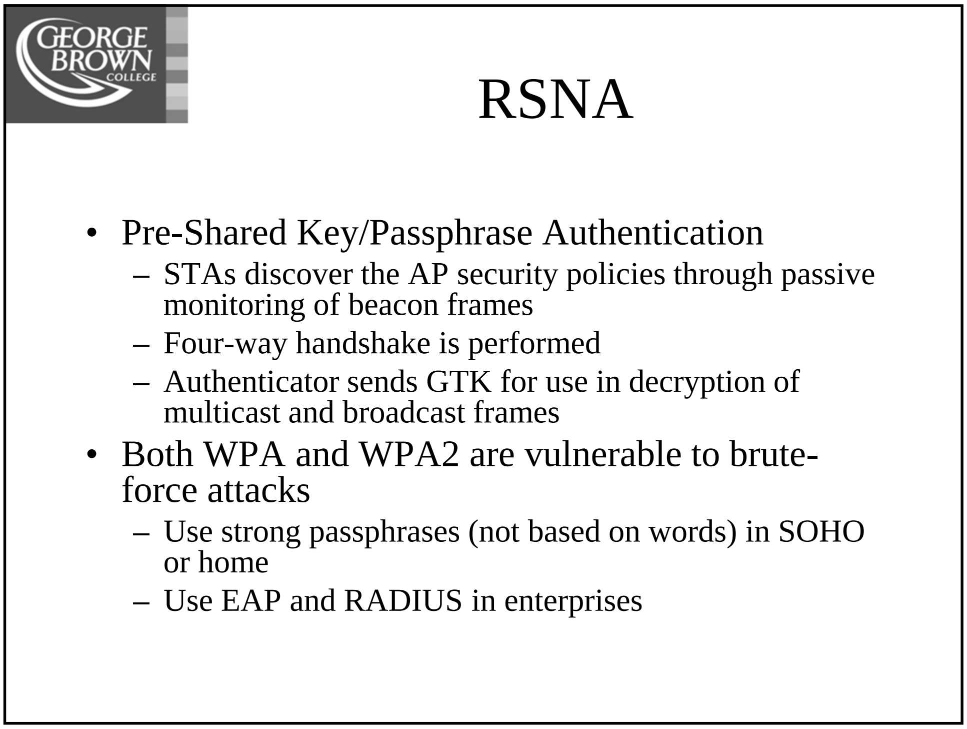
RSNA

- IEEE 802.1X Authentication and Key Management (AKM)
  - Port-based authentication
  - STAs must have port access entity (PAE)
  - No specific authentication type
  - Includes:
    - Authenticaton roles
    - Controlled and uncontrolled ports
    - IEEE 802.1X generic authentication flow framework



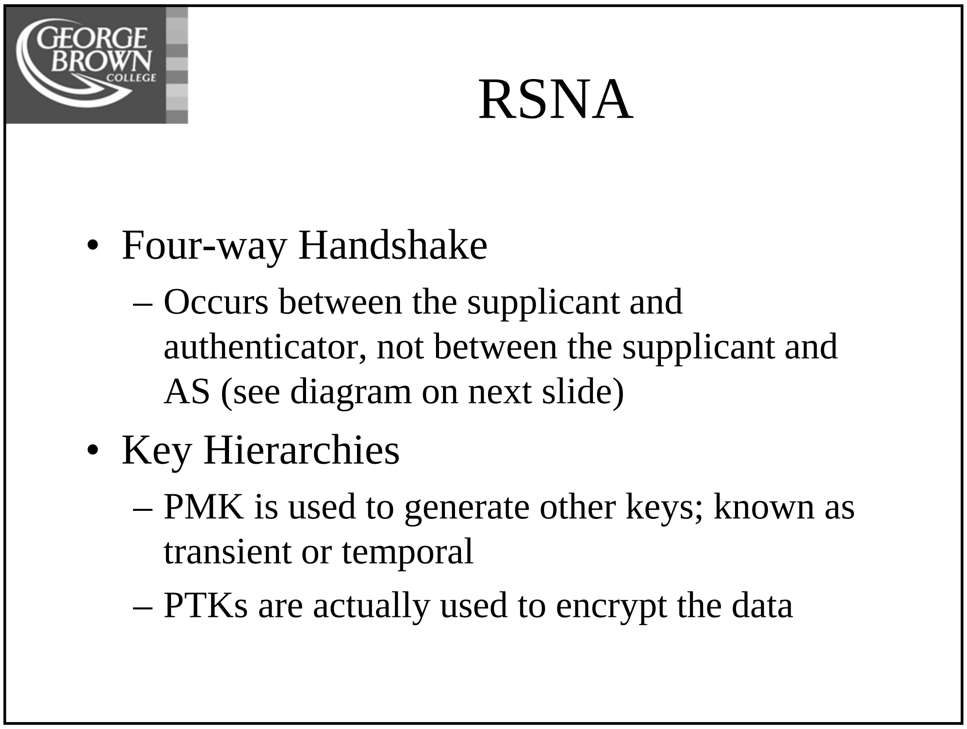
RSNA

- IEEE 802.1X (cont’d.)
  - Authentication Roles
    - Supplicant, Authenticator & Authentication Server
    - AS is most frequently RADIUS
  - Controlled and Uncontrolled Ports
    - Controlled ports do not pass data traffic until device is authenticated over an uncontrolled port
  - Generic Authentication Flow Framework
    - Essentially EAP



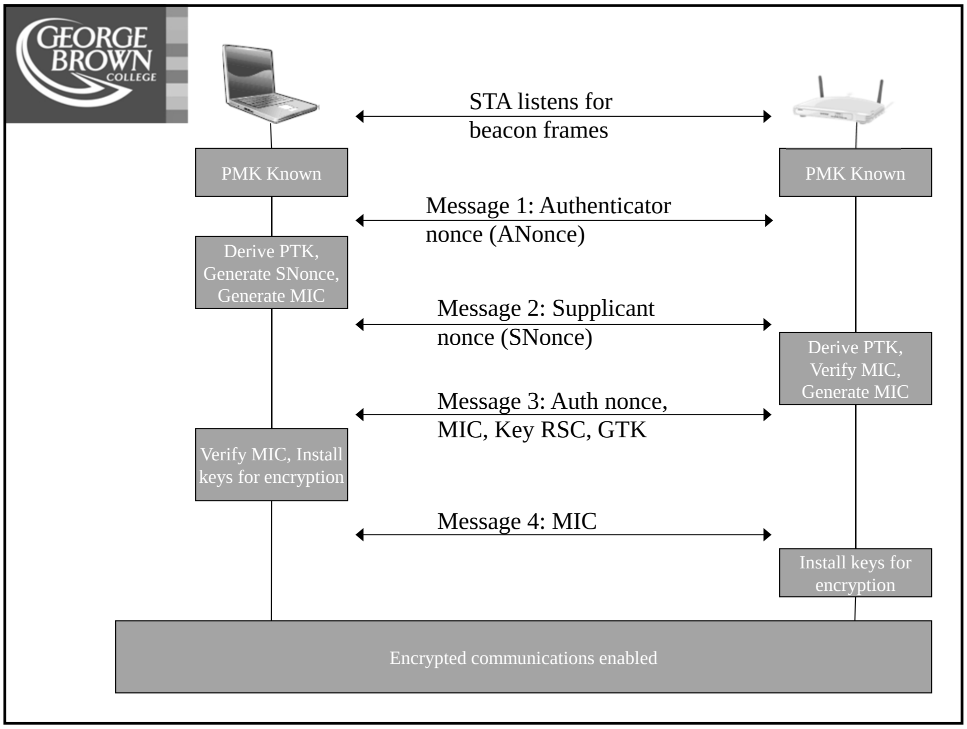
RSNA

- Pre-Shared Key/Passphrase Authentication
  - – STAs discover the AP security policies through passive monitoring of beacon frames
  - – Four-way handshake is performed
  - – Authenticator sends GTK for use in decryption of multicast and broadcast frames
- Both WPA and WPA2 are vulnerable to brute-force attacks
  - – Use strong passphrases (not based on words) in SOHO or home
  - – Use EAP and RADIUS in enterprises



RSNA

- Four-way Handshake
  - – Occurs between the supplicant and authenticator, not between the supplicant and AS (see diagram on next slide)
- Key Hierarchies
  - – PMK is used to generate other keys; known as transient or temporal
  - – PTKs are actually used to encrypt the data



STA listens for beacon frames

PMK Known

PMK Known

Message 1: Authenticator nonce (ANonce)

Derive PTK, Generate SNonce, Generate MIC

Message 2: Supplicant nonce (SNonce)

Derive PTK, Verify MIC, Generate MIC

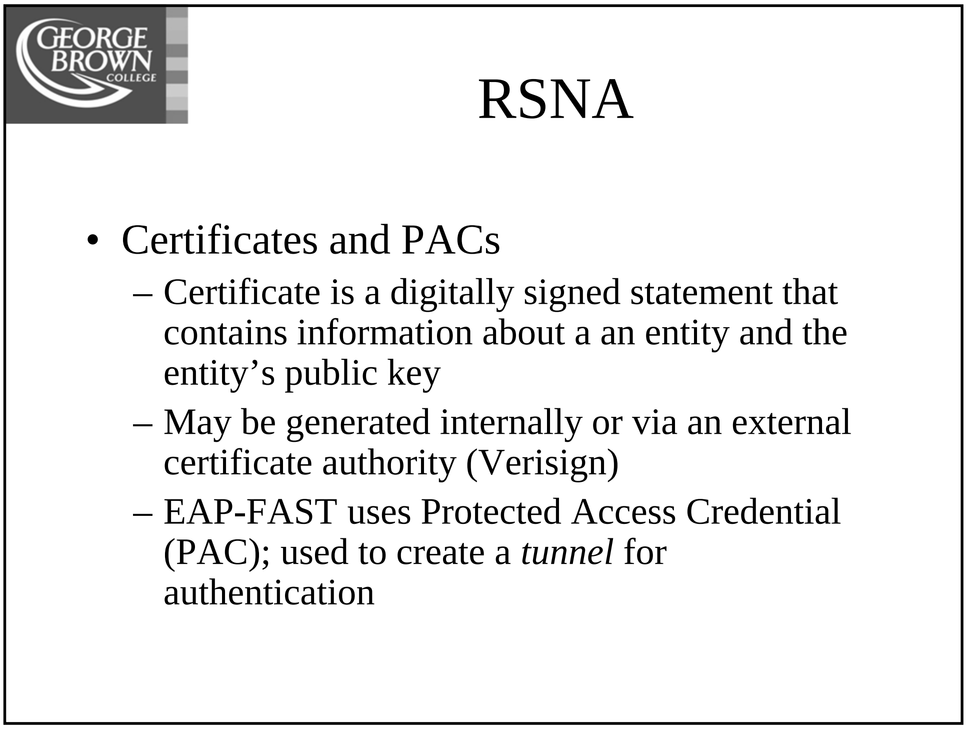
Message 3: Auth nonce, MIC, Key RSC, GTK

Verify MIC, Install keys for encryption

Message 4: MIC

Install keys for encryption

Encrypted communications enabled



RSNA

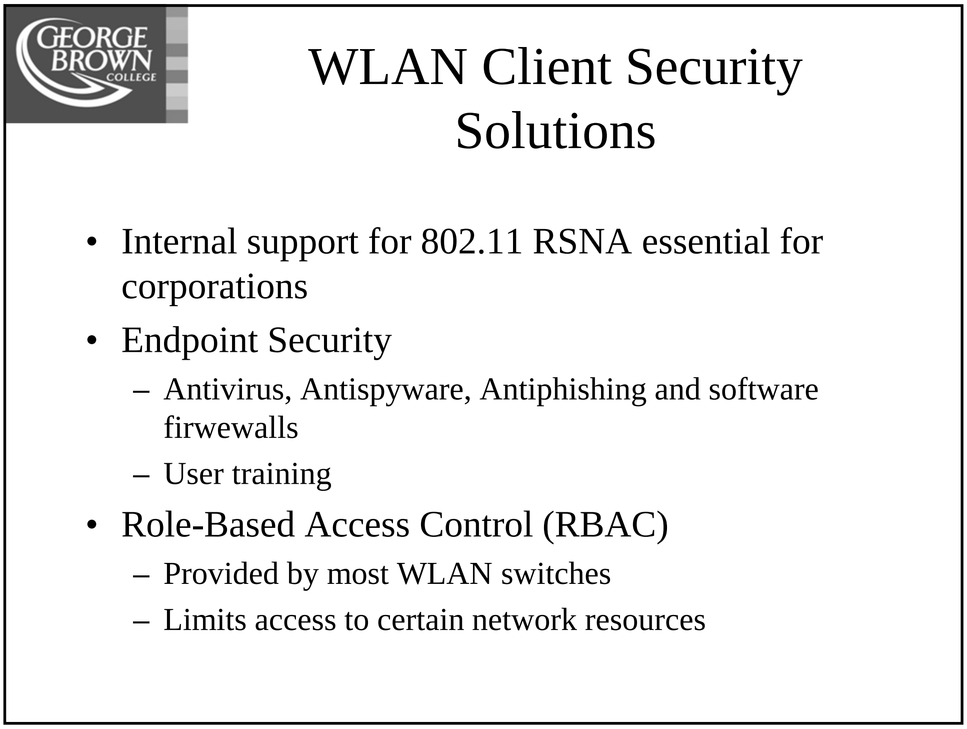
- Certificates and PACs
  – Certificate is a digitally signed statement that contains information about a an entity and the entity’s public key
  – May be generated internally or via an external certificate authority (Verisign)
  – EAP-FAST uses Protected Access Credential (PAC); used to create a *tunnel* for authentication

RSNA

- Transition Security Network
  - A network that allows pre-RSNA and RSNA security associations
  - Supports older WEP and new TKIP and CCMP at the same time

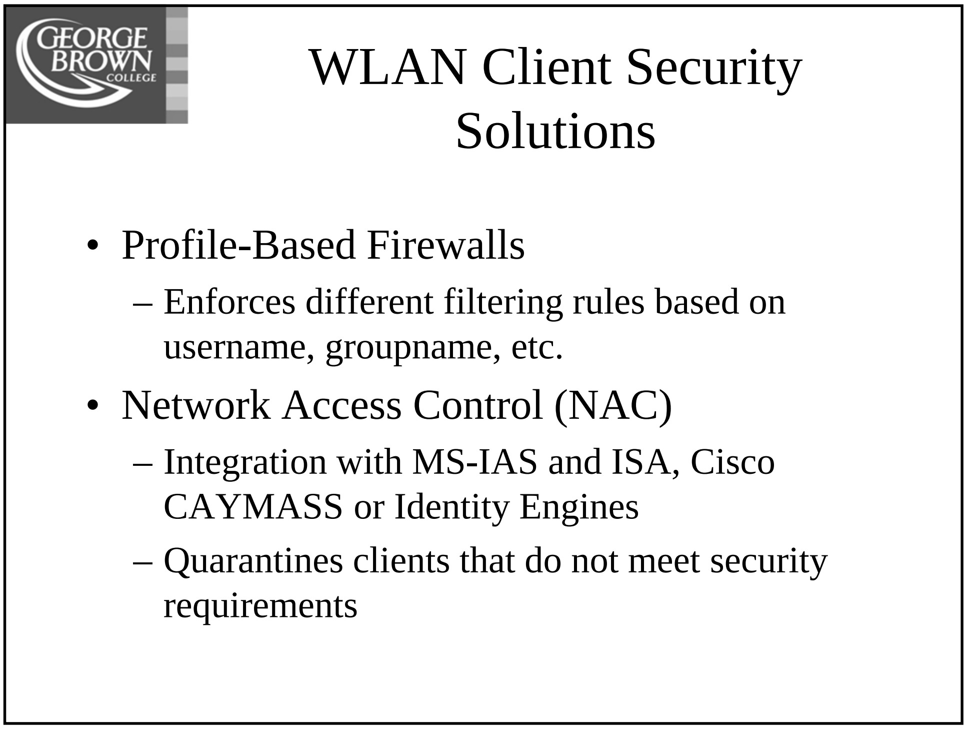
AAA Security Components

- EAP Types
  - EAP MD5, LEAP, EAP-TLS, PEAP, EAP-FAST
- RADIUS – Remote Authentication Dial-In User Service
  - Can use MS-CHAP with Active Directory
- Learn Common Terms from page 497, Table 10.2



WLAN Client Security Solutions

- Internal support for 802.11 RSNA essential for corporations
- Endpoint Security
  - Antivirus, Antispyware, Antiphishing and software firwewalls
  - User training
- Role-Based Access Control (RBAC)
  - Provided by most WLAN switches
  - Limits access to certain network resources



WLAN Client Security Solutions

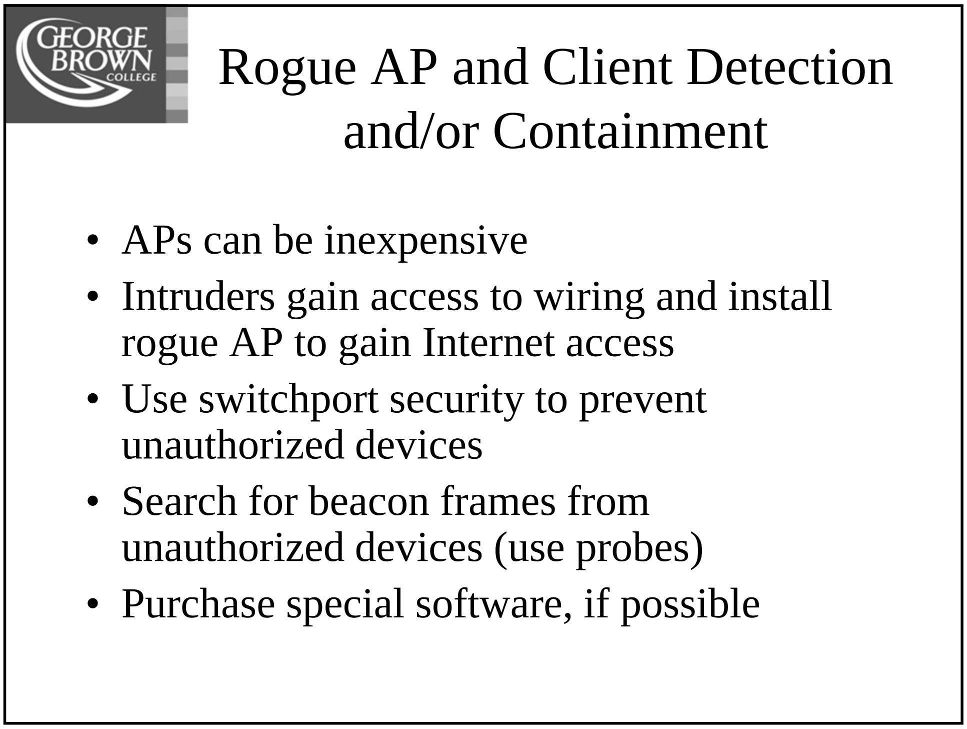
- Profile-Based Firewalls
  - Enforces different filtering rules based on username, groupname, etc.
- Network Access Control (NAC)
  - Integration with MS-IAS and ISA, Cisco CAYMASS or Identity Engines
  - Quarantines clients that do not meet security requirements

WLAN Client Security Solutions

- Client Portals/Web Authentication
  - Traffic coming through AP is initially directed to an access control device
  - Can be foiled by Proxy Websites

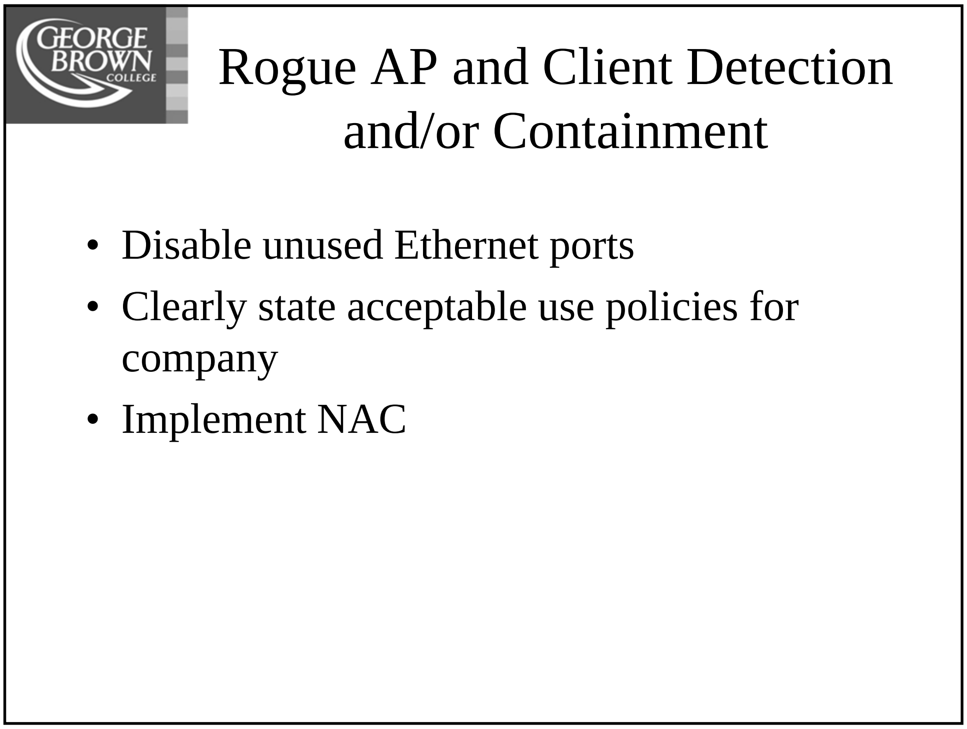
WLAN System Security and Management

- Use SNMP v3 is possible, with AES encryption
- HTTPS only
- SSH2 for network console access



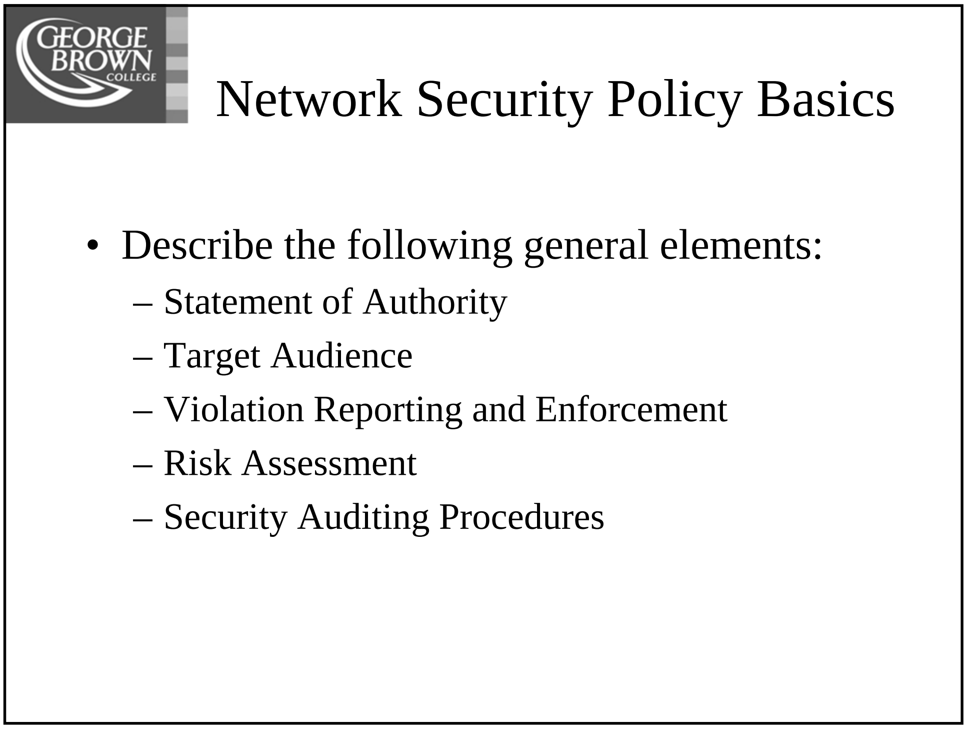
Rogue AP and Client Detection and/or Containment

- APs can be inexpensive
- Intruders gain access to wiring and install rogue AP to gain Internet access
- Use switchport security to prevent unauthorized devices
- Search for beacon frames from unauthorized devices (use probes)
- Purchase special software, if possible



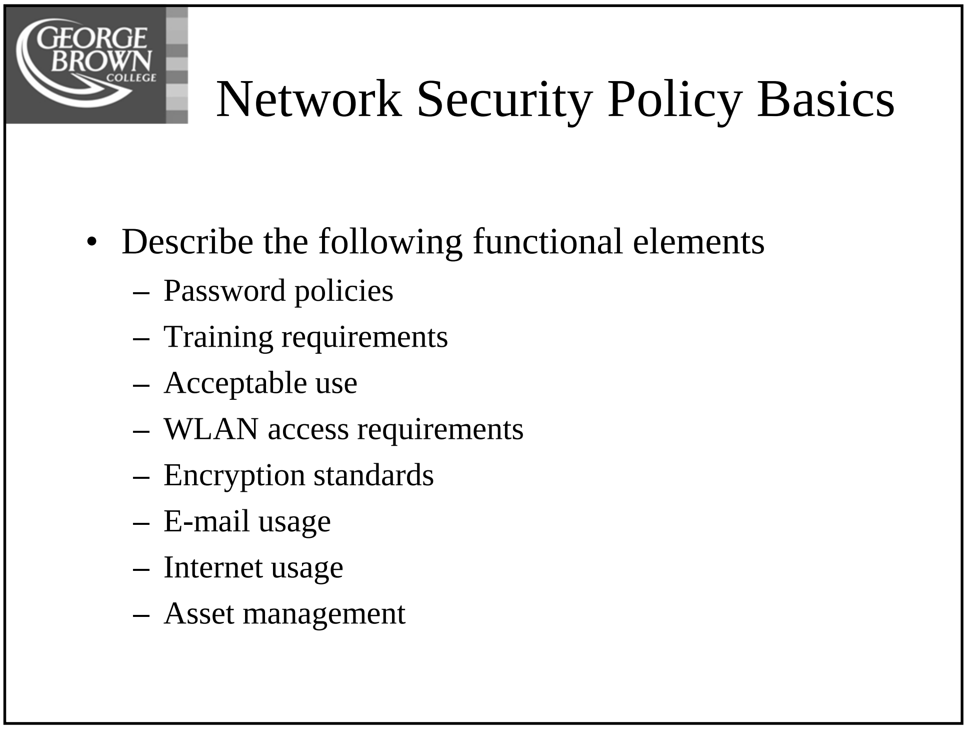
Rogue AP and Client Detection and/or Containment

- Disable unused Ethernet ports
- Clearly state acceptable use policies for company
- Implement NAC



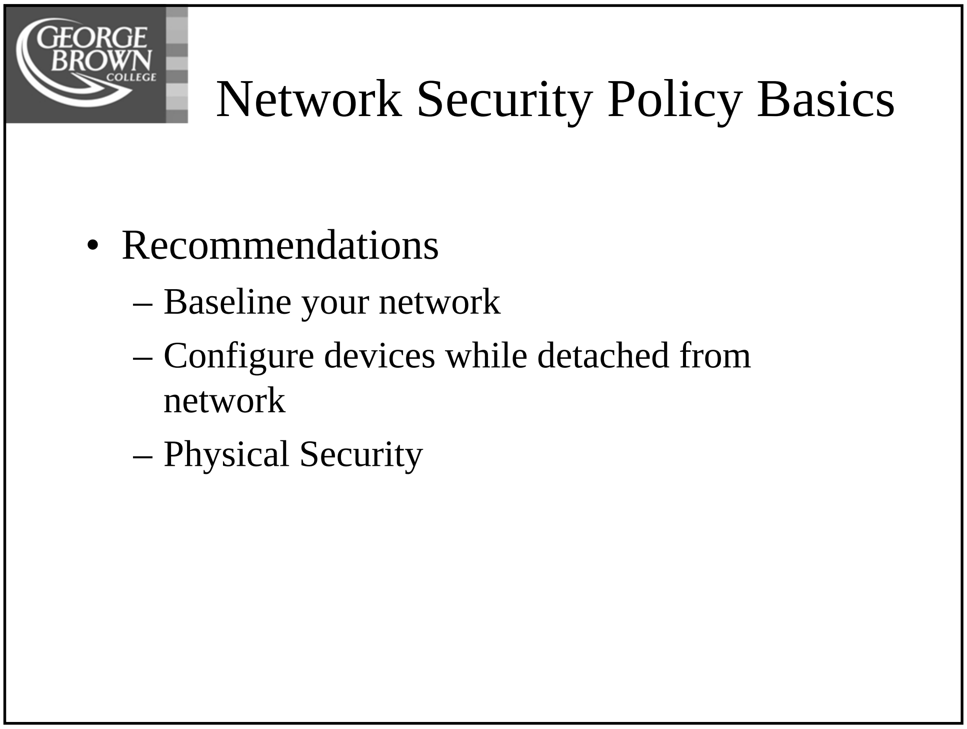
Network Security Policy Basics

- Describe the following general elements:
  - Statement of Authority
  - Target Audience
  - Violation Reporting and Enforcement
  - Risk Assessment
  - Security Auditing Procedures



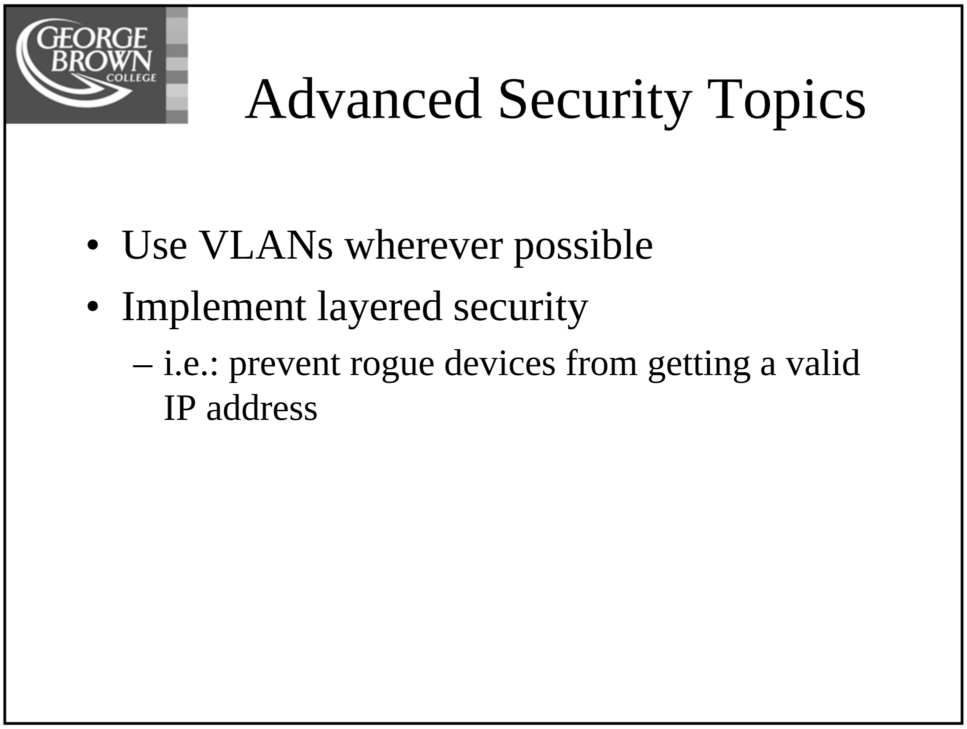
Network Security Policy Basics

- Describe the following functional elements
  - Password policies
  - Training requirements
  - Acceptable use
  - WLAN access requirements
  - Encryption standards
  - E-mail usage
  - Internet usage
  - Asset management



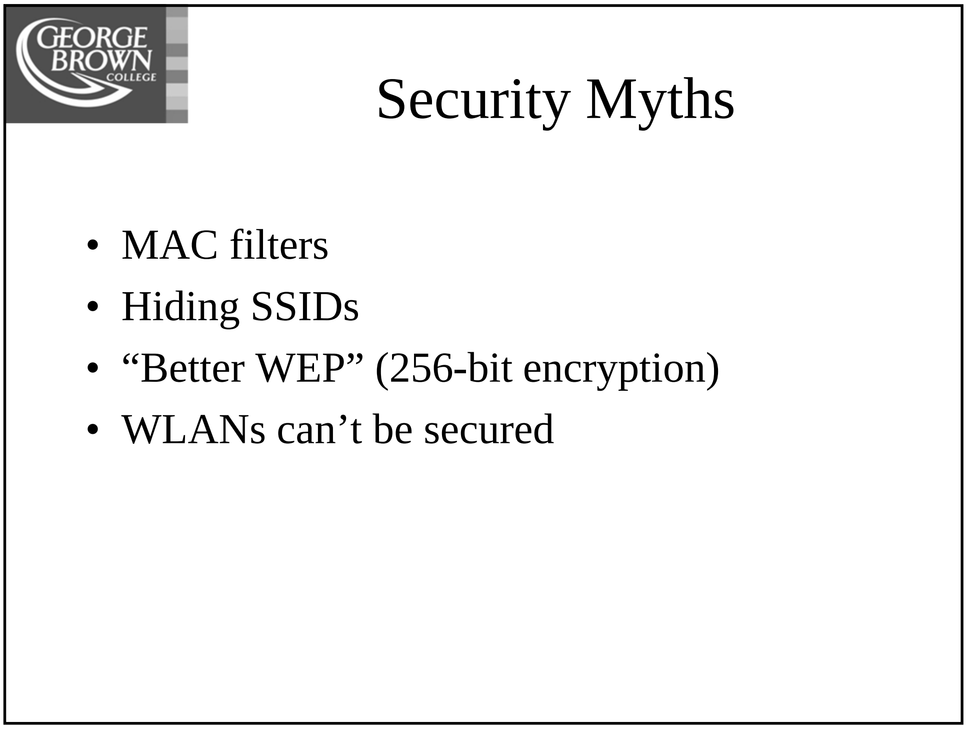
Network Security Policy Basics

- Recommendations
  - – Baseline your network
  - – Configure devices while detached from network
  - – Physical Security



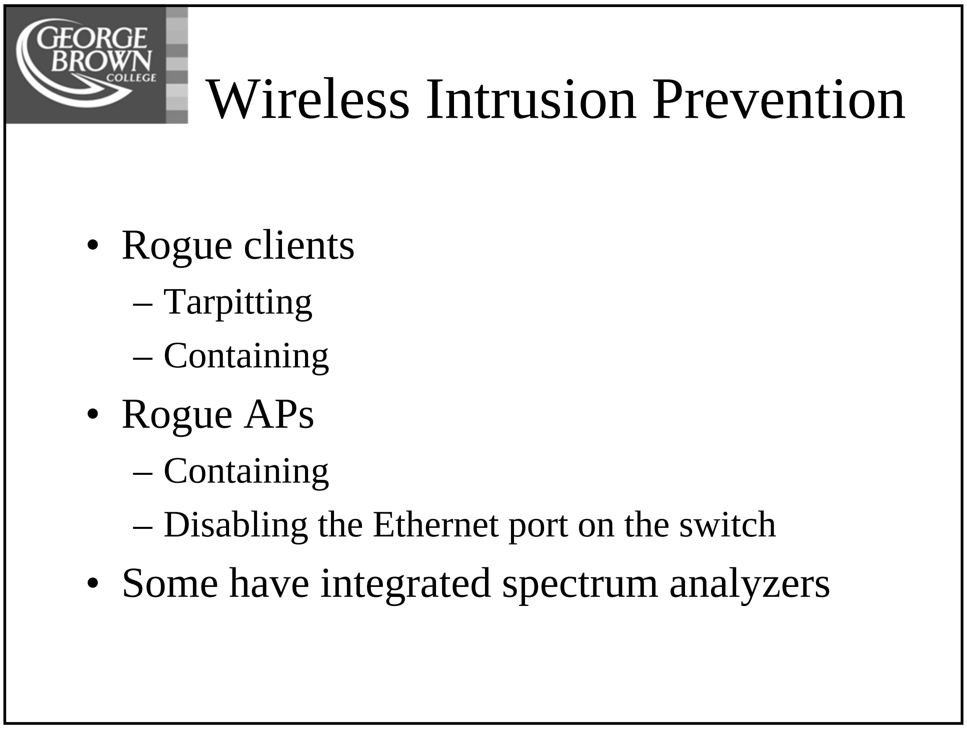
Advanced Security Topics

- Use VLANs wherever possible
- Implement layered security
  - – i.e.: prevent rogue devices from getting a valid IP address



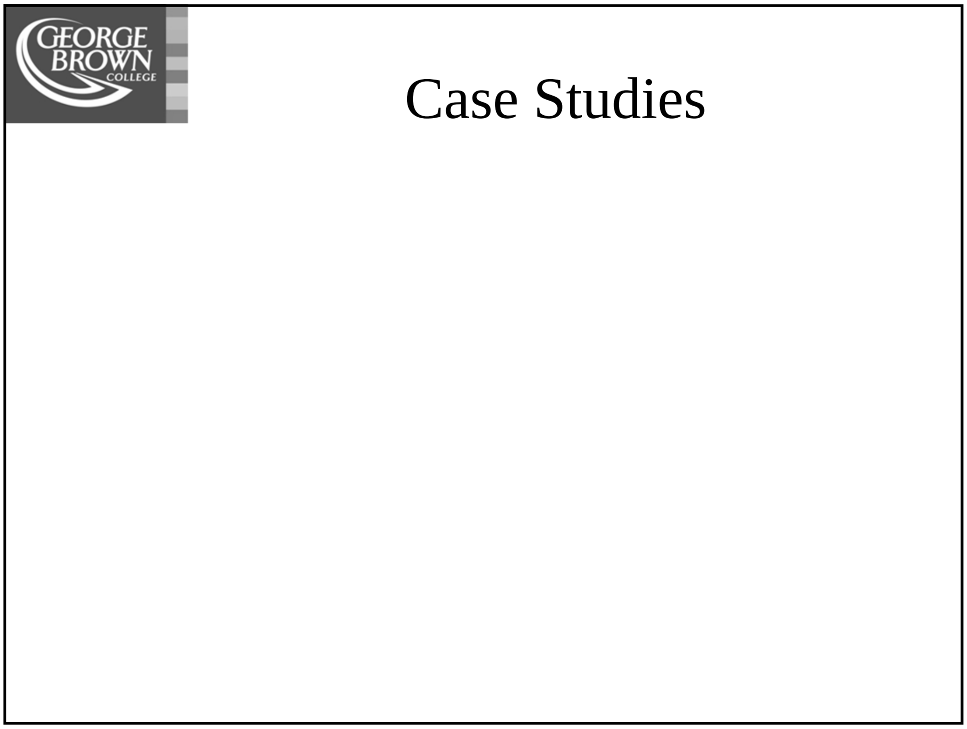
Security Myths

- MAC filters
- Hiding SSIDs
- “Better WEP” (256-bit encryption)
- WLANs can’t be secured



Wireless Intrusion Prevention

- Rogue clients
  - Tarpitting
  - Containing
- Rogue APs
  - Containing
  - Disabling the Ethernet port on the switch
- Some have integrated spectrum analyzers



Case Studies