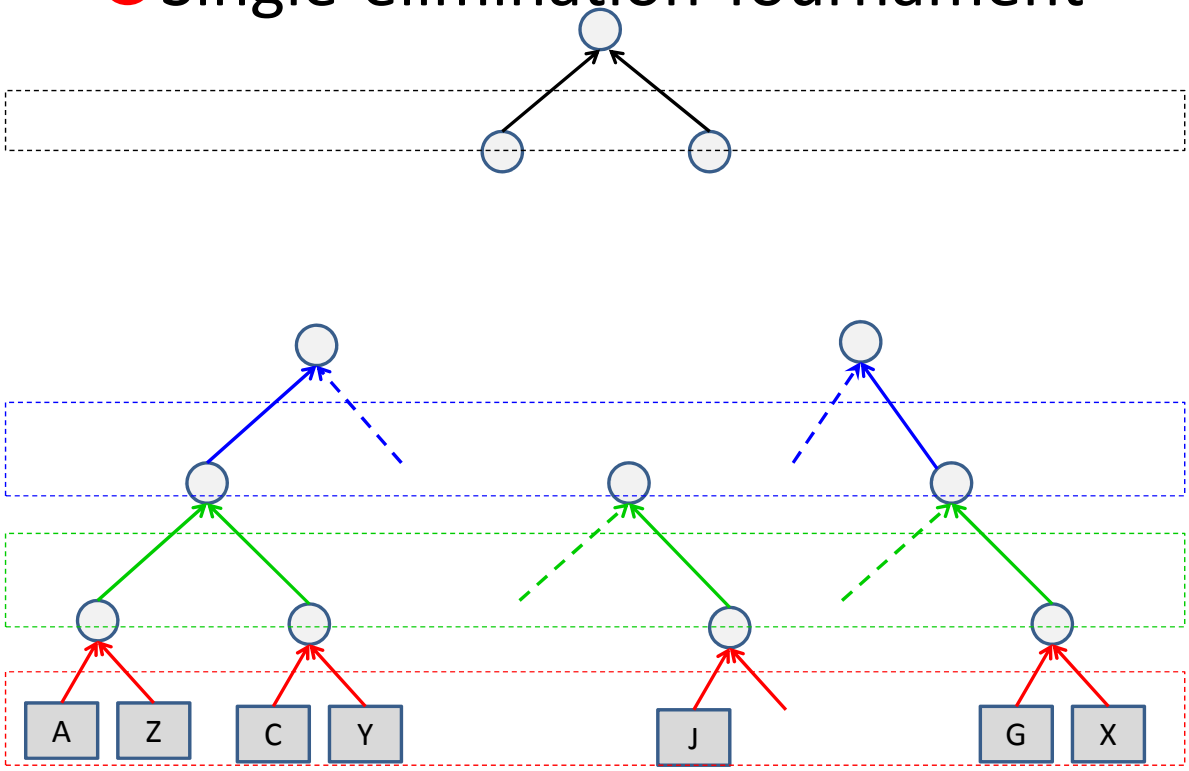
2015 Summer Camp: Wireless LAN Security Exercises

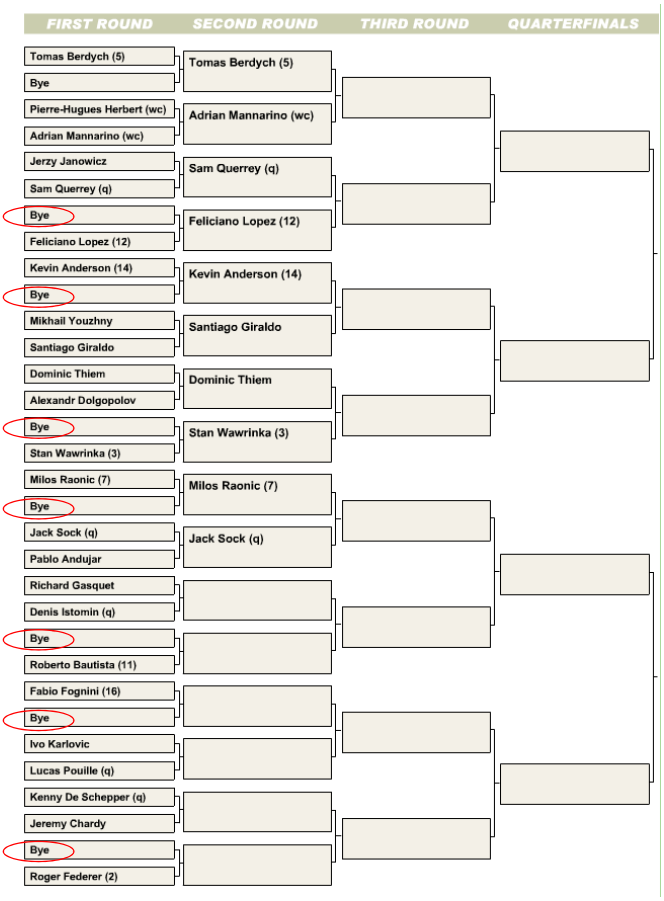
2015 JMU Cyber Defense Boot Camp

How Many Matches are Needed?

- Tennis fan?
  - Wimbledon Open (began on Monday June 29th, 2015)
- 125 players
- The championship is organized in rounds
  - In each round, players are paired and a match is played
    - Winner goes to next round
    - Loser exits
- $125 \neq 2^x \Rightarrow$ some guys get a bye in the first round
  - No matches!
- Question
  - ❶ How many matches are needed to decide a champion?

❷Single-elimination Tournament





125 players

How many matches?

Simpler solution?

Simple Solution!

- Simplicity is important for security too
  - Complexity is big enemy for security
- Too complex security solutions?
  - People will give up
  - People will bypass
- Effective security measures?
  - "As simple as possible, but not simpler"
  - Simple for developers
  - Simple for end users
- Cybersecurity principle #9

Questions on Wireless LAN (1/2)

- Have you **used** a wireless local area network before?
  - At home?
  - At work?
  - With your cell phone?
- Have you **configured** a wireless AP before?
- Which one do you use, WEP, WPA, or WPA2?
  - How secure is it?
  - Why?

Questions on Wireless LAN (2/2)

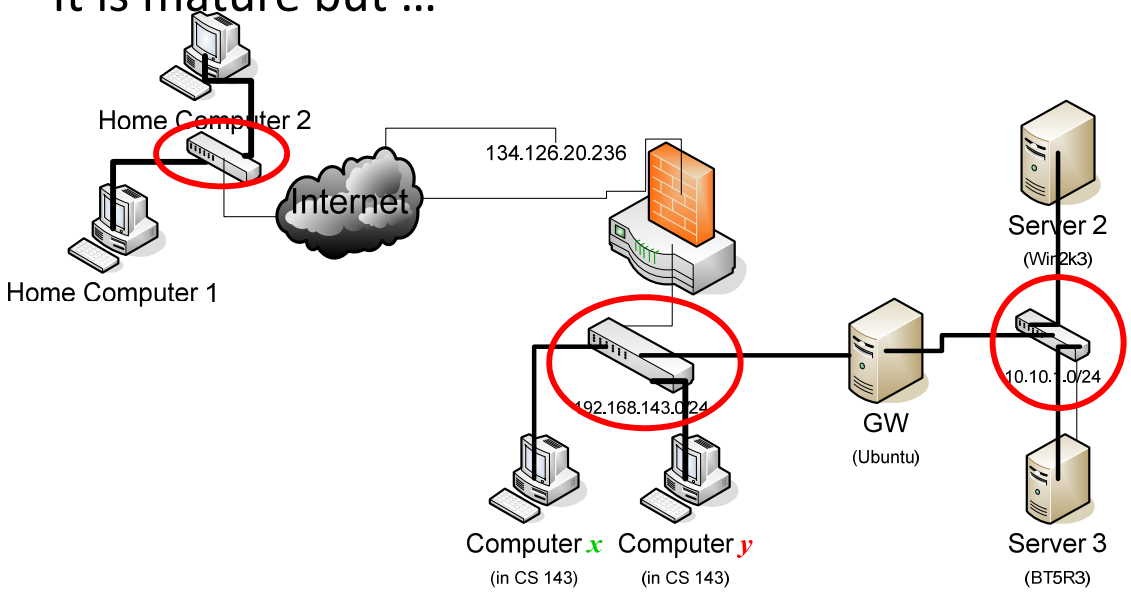
- Have you heard these terminologies before?
  - WiFi (Wireless Fidelity)
  - Wireless access point (AP)
  - Service set identification (SSID)
  - Hot spots, evil twins
  - WEP (Wired Equivalent Privacy)
  - WPA (Wireless Protected Access)
    - WPA-PSK (Pre-Shared Key)
  - WPA2

Use different algorithms

Evolved over years

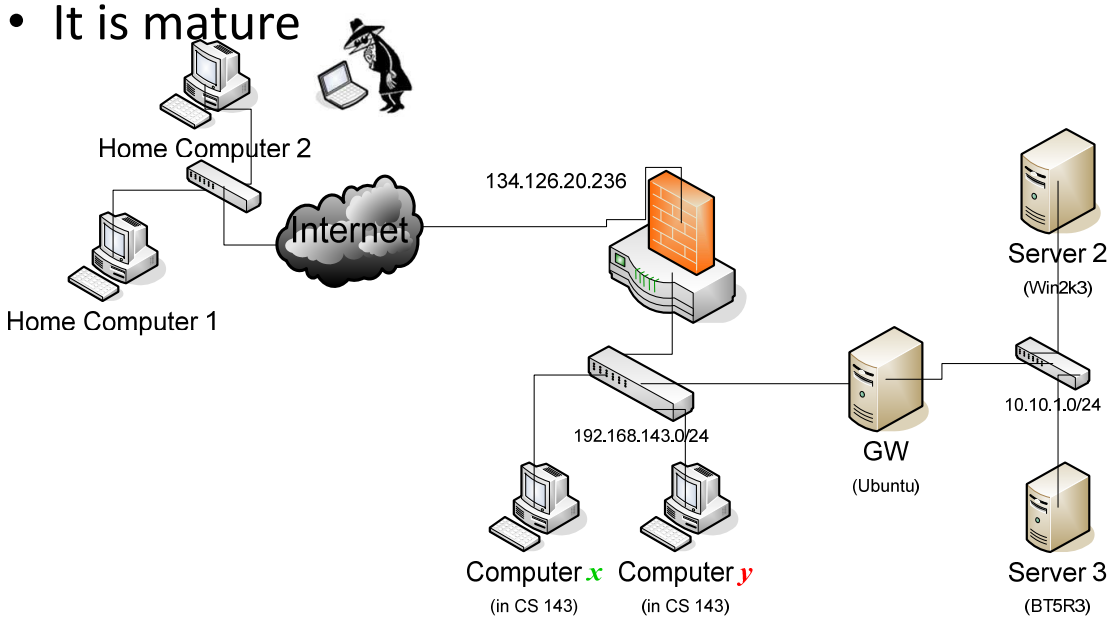
Wired Computer Networks

- It is mature but …

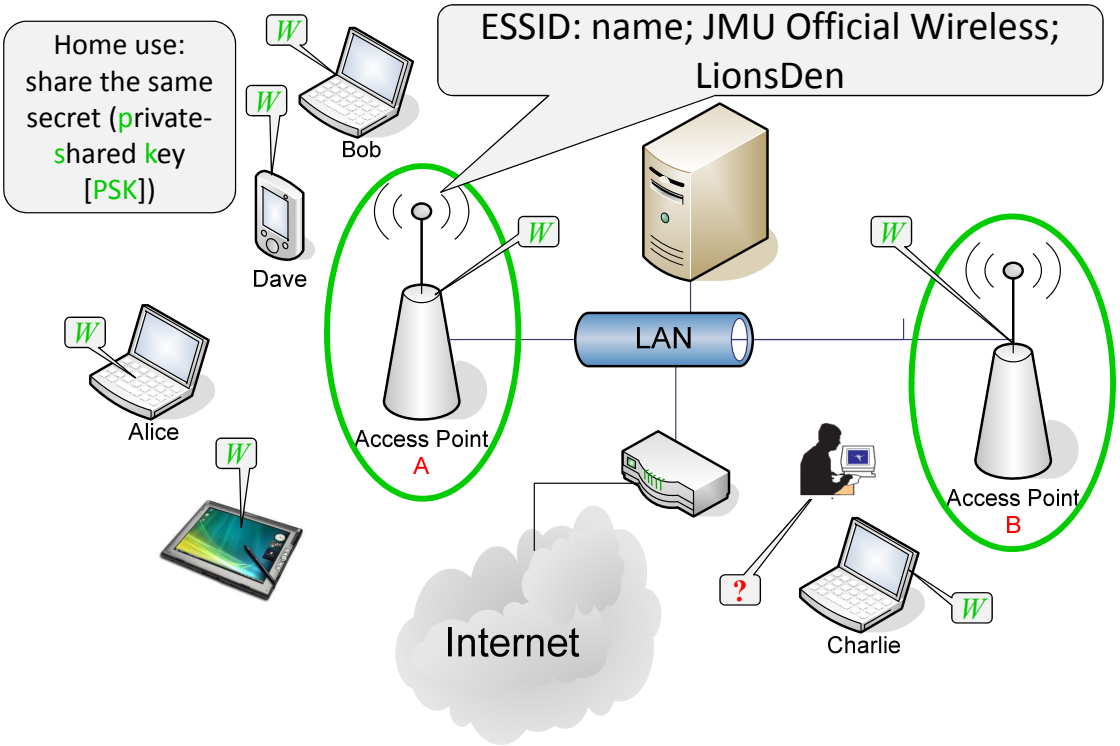


Wired Computer Network: Inconvenience

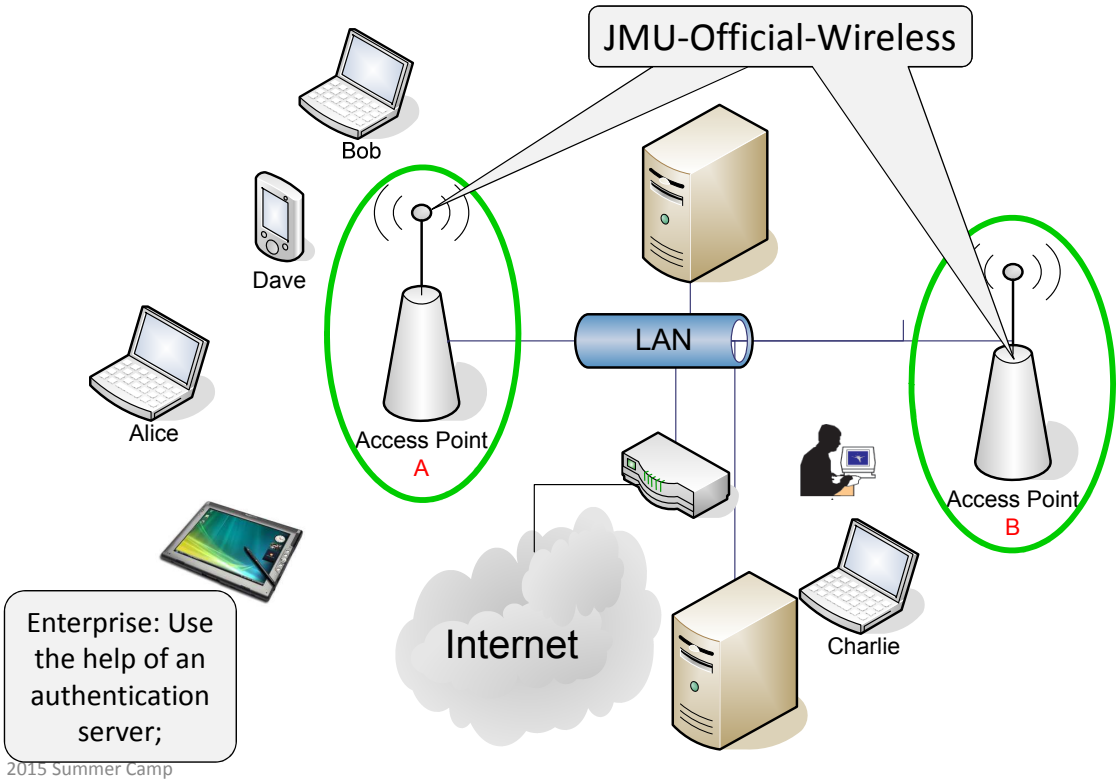
- It is mature



Wireless Would be Nice



Wireless Would be Nice

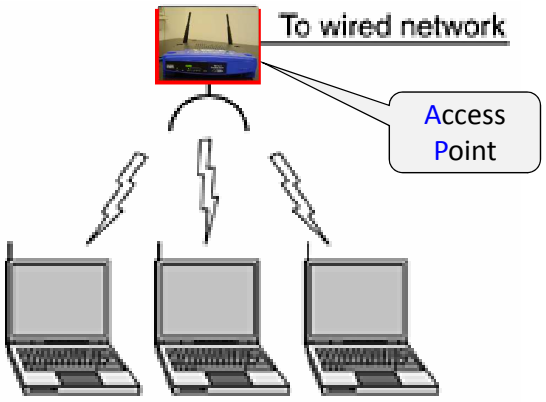


Hardware?

Wireless Access Point (AP)

Wireless card (WiFi adapter card)

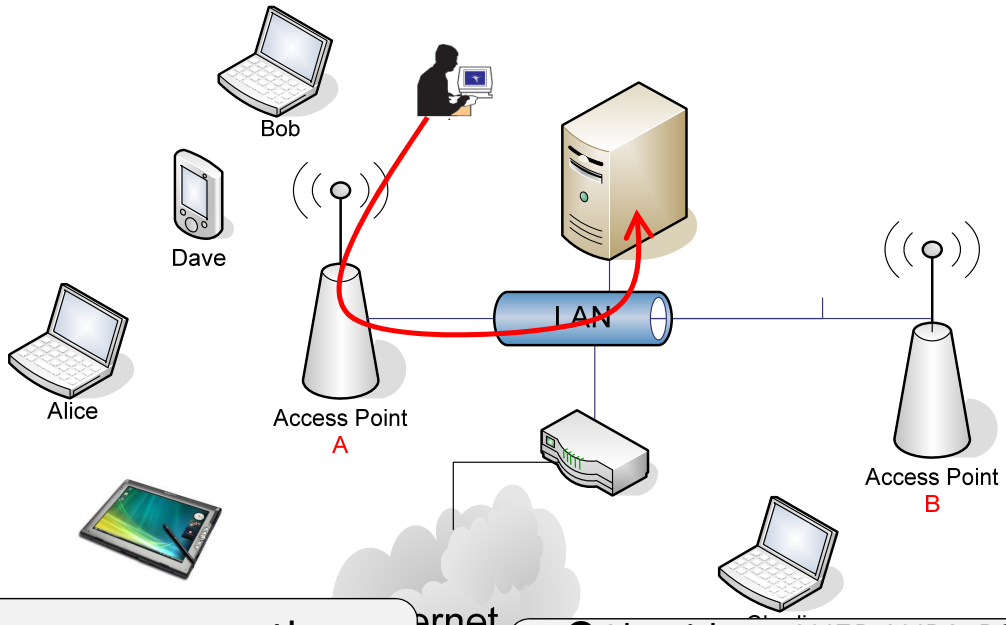
Wireless LAN Topology



① Independent Basic Service Set (BSS, IBSS): ad hoc mode (independent, peer-to-peer): no access point

② Extended Service Set (ESS): use AP; Infrastructure mode: one access point manages; greater range

Typical Wireless LAN Configuration



How secure are these configurations?

❶Algorithms: WEP, WPA-PSK, WPA2
❷Shared key: how long?

Organization

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

We will work on captured traffic, not live traffic [airodump]

Take longer

Road Map

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

Step 0

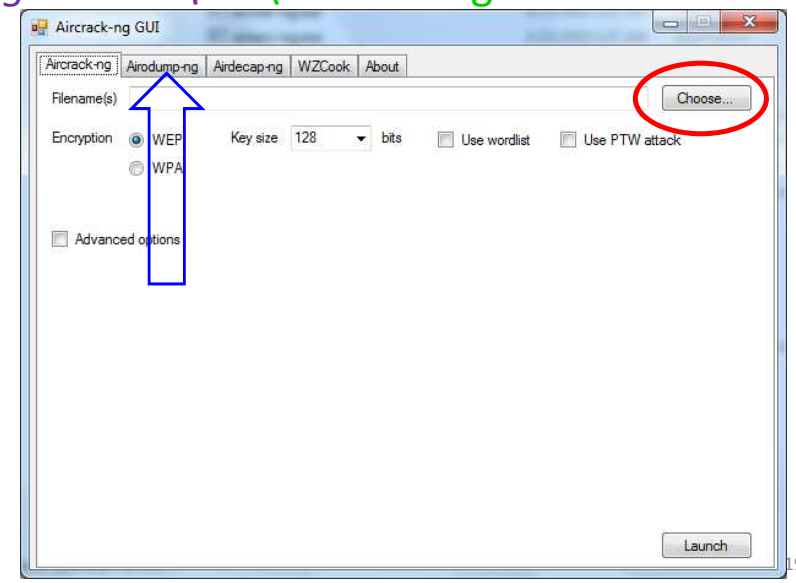
- Run Firefox to log into your vCenter server and find your Windows 2003 VM
- Use the "**WLAN and Crypto Security**" VM snapshot

Aircrack-ng for Windows (1/2)

- It has aircrack-ng for Windows
  - You can download it http://www.aircrack-ng.org/doku.php?id=main

Aircrack-ng for Windows (2/2)

- Run c:\wireless\wireless*aircrack-ng-1.1-win**aircrack-ng-1.1-win*\bin\Aircrack-ng GUI.exe
- (You can also run it directly from a shortcut on your Desktop)



Exercises

- In this unit, we will crack some real-world wireless local area networks with traffic captured in files
  - Not live traffic
- These traffic packets were captured with Wireshark

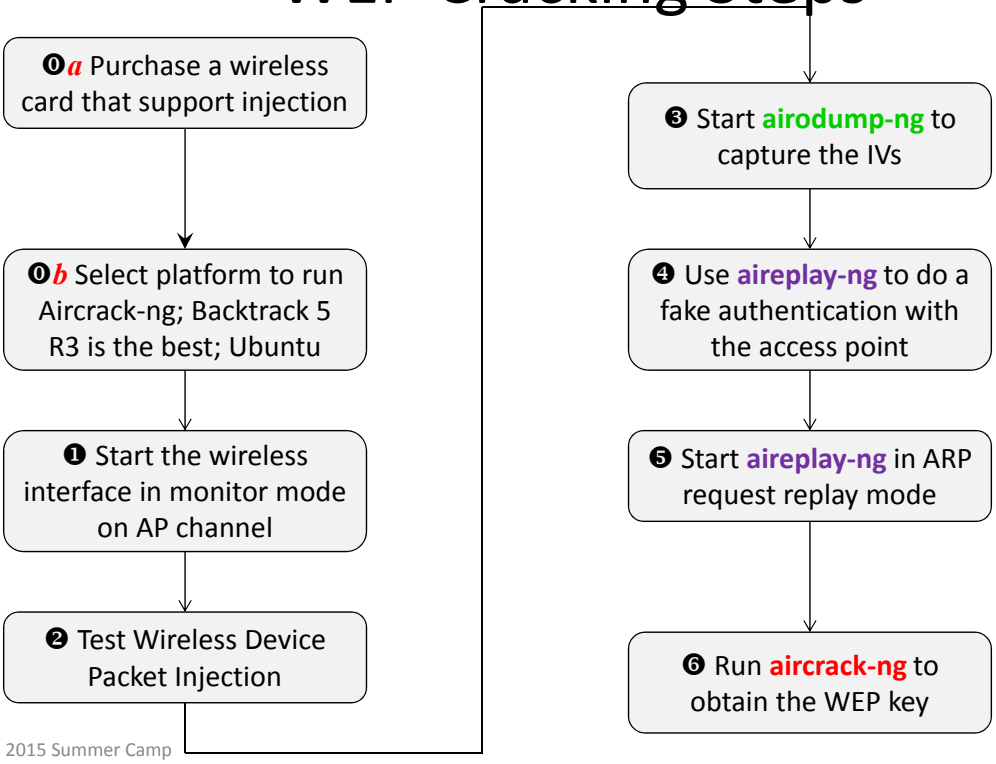
Road Map

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

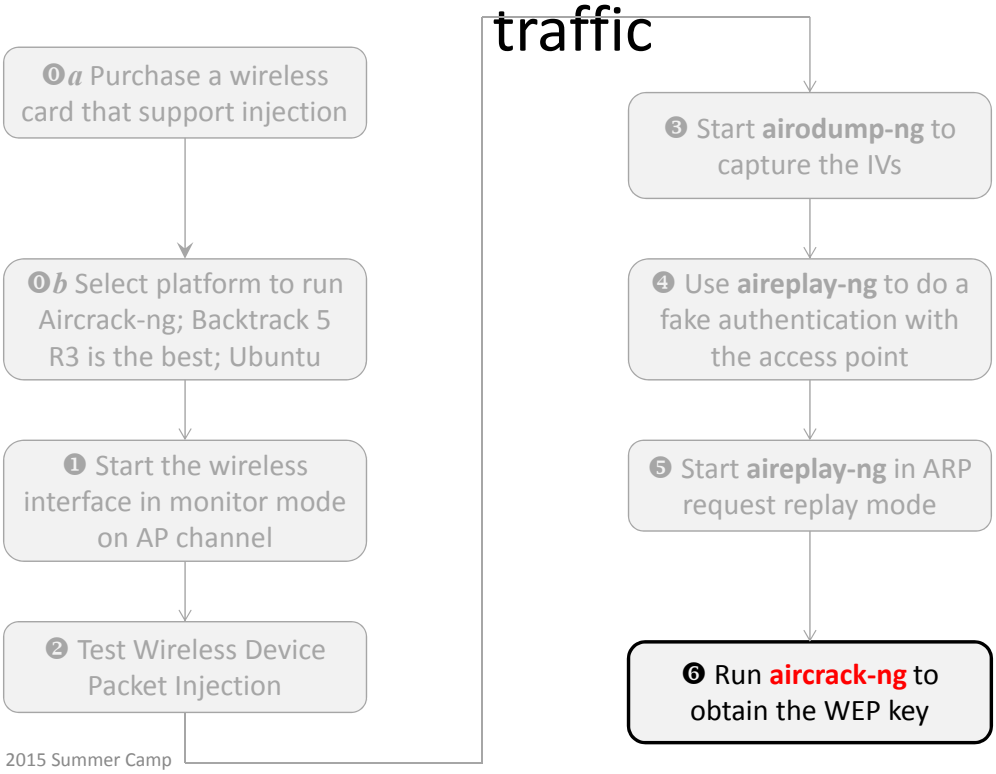
Task ①: WEP Cracking

- The target wireless network is using WEP

WEP Cracking Steps

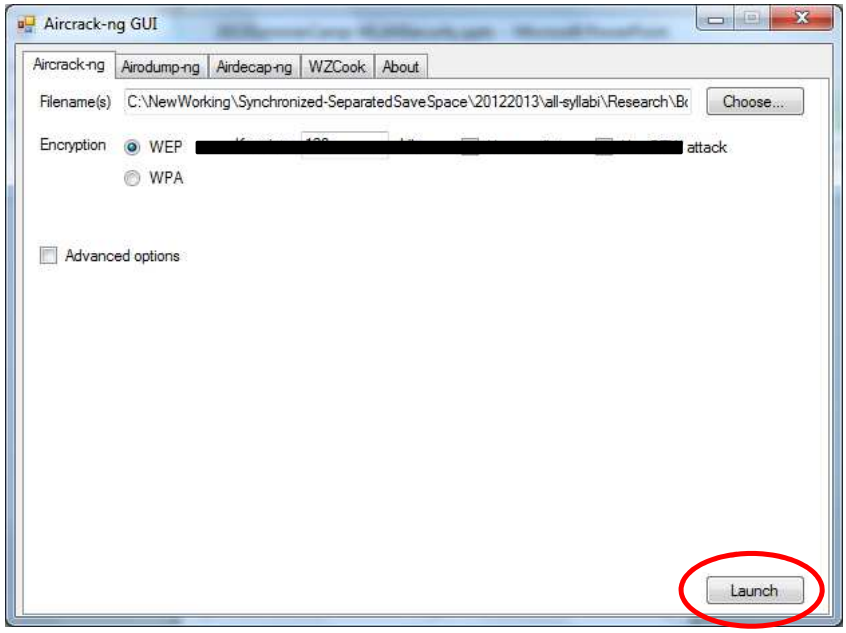


WEP Cracking Steps with captured traffic



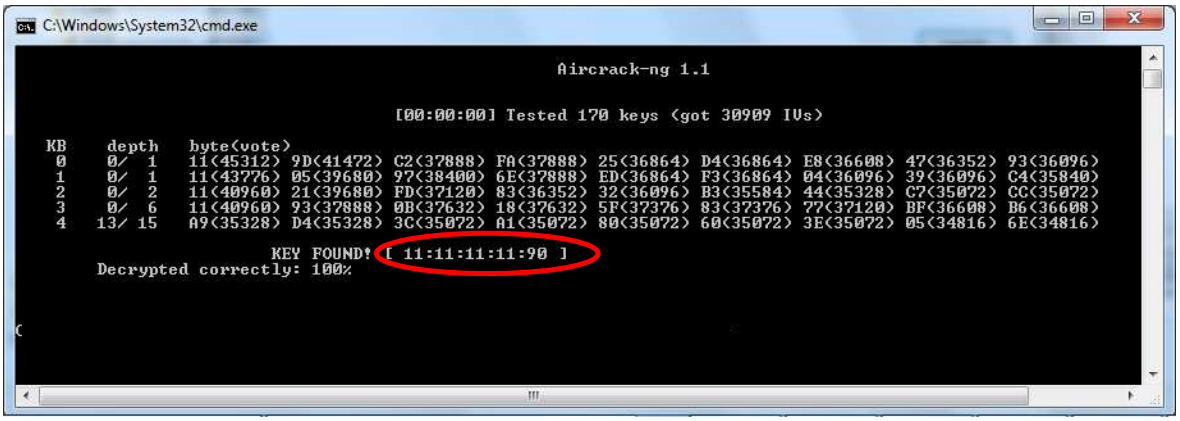
Task ①: WEP Cracking

- Filename(s) c:\wireless\wireless\WEPFile01\wep3-01.cap



What did you get?

- Mine



Now, close Aircrack-ng GUI.exe

Now What?

- You can use the cracked WEP key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

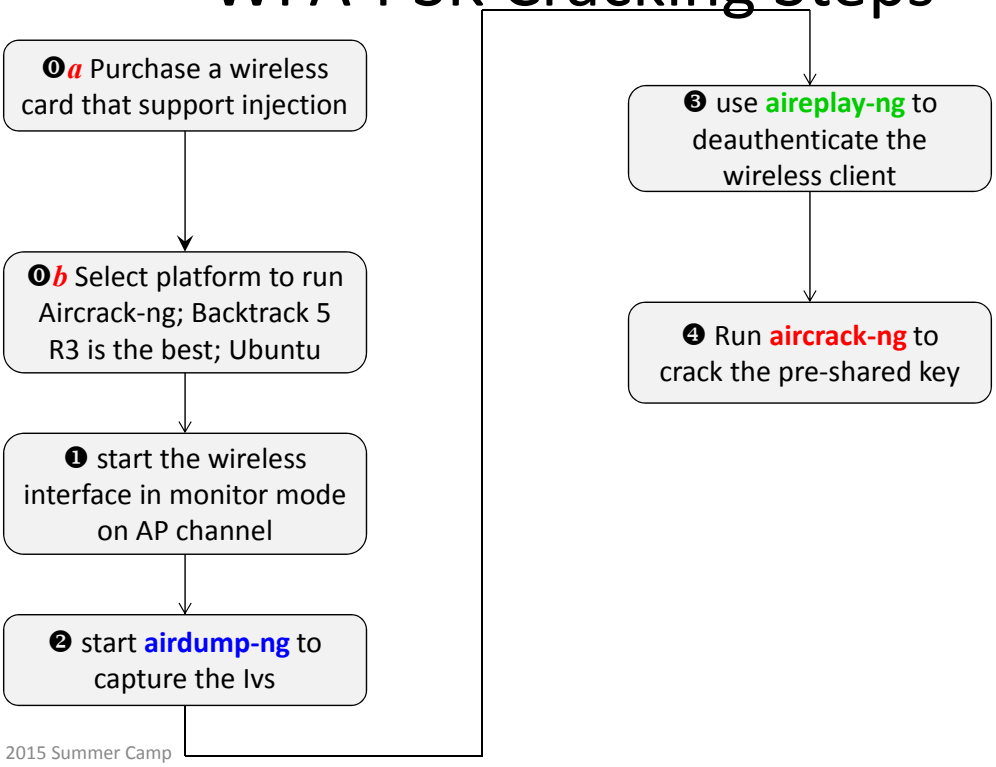
Road Map

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

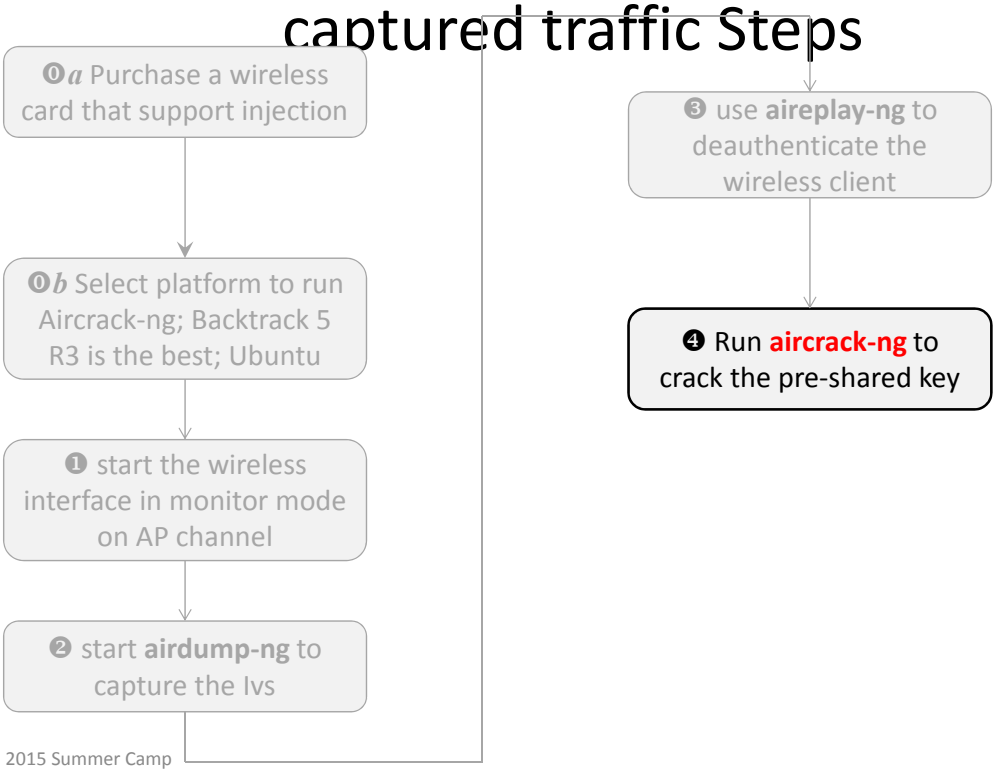
Task ②: WPA-PSK Cracking

- The target wireless network is using WPA-PSK

WPA-PSK Cracking Steps

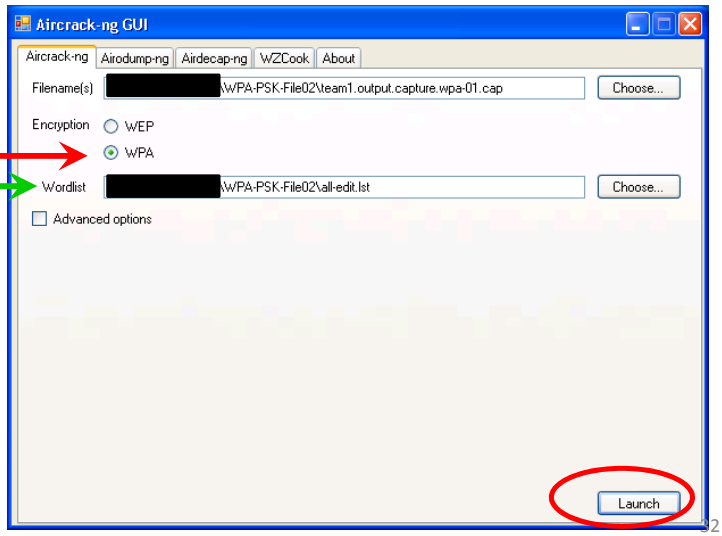


Task ②: WPA-PSK Cracking with captured traffic Steps



Task ②: WPA-PSK Cracking

- Filename(s): c:\wireless\wireless\WPA-PSK-File02\team1.output.capture.wpa-01.cap
- Wordlist: c:\wireless\wireless\WPA-PSK-File02\all-edit.lst
  - Do **not** use all.lst



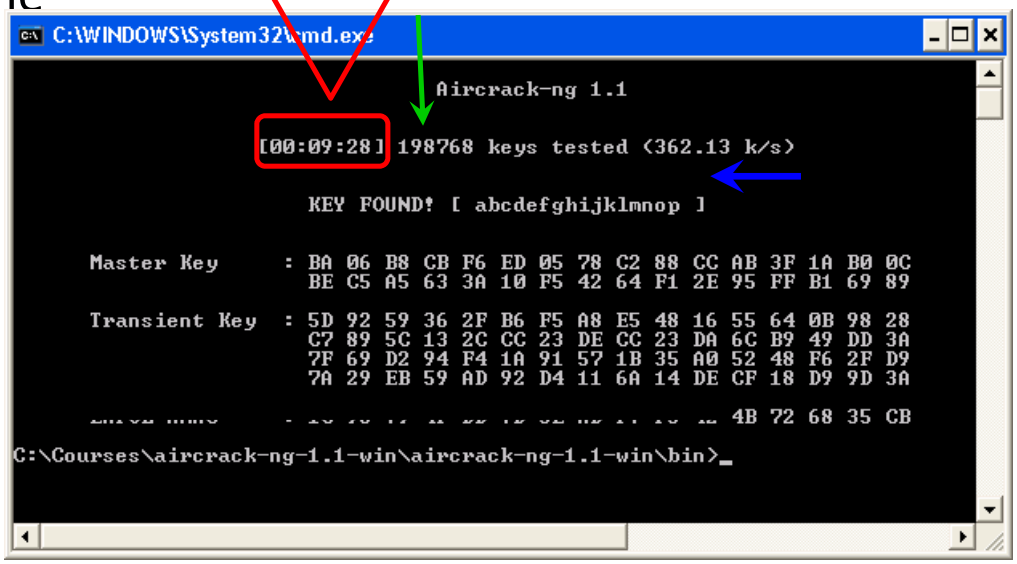
Task ②: WPA-PSK Cracking

- Choose index 2 if you get prompted

Task ②: What did you get?

This is almost 10 minutes

- Mine



Now, close Aircrack-ng GUI.exe

Now What?

- You can use the cracked WPA-PSK key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

Road Map

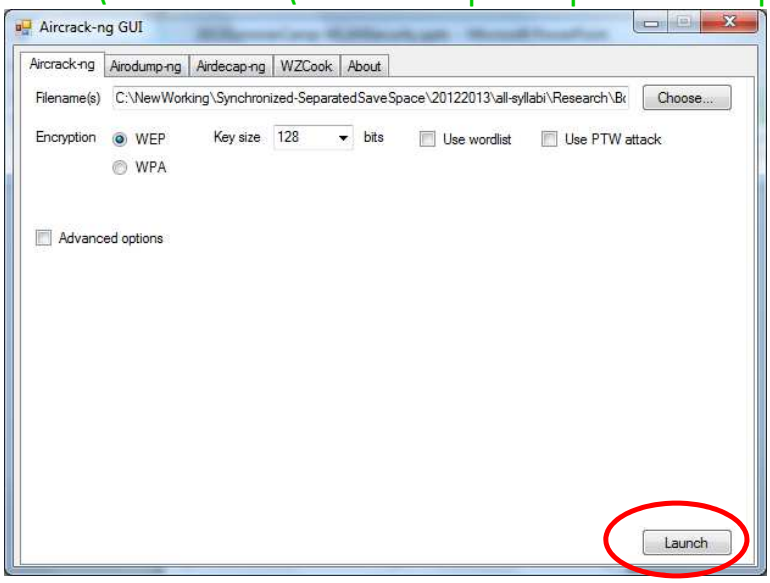
- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

Task ③: WEP Cracking

- The target wireless network is using WEP

Task ③: WEP Cracking – File 3

- Filename(s)
  c:\wireless\wireless\WEPFile03\team4.output.capture-03.cap

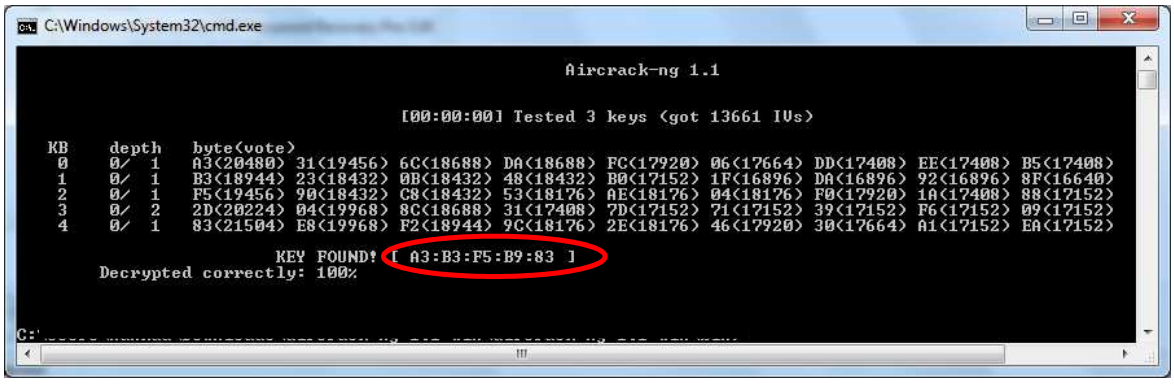


Task ③: WEP Cracking – File 3

- Choose index 2 if you get prompted

What did you get?

- Mine



Now, close Aircrack-ng GUI.exe

Now What?

- You can use the cracked WEP key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

Everybody likes a quiz

- Which of the following wireless security algorithms are not considered weak:
  a) WEP
  b) WPA-PSK
  c) WPA2
  d) WPA-TKIP
  e) None of the above

Road Map

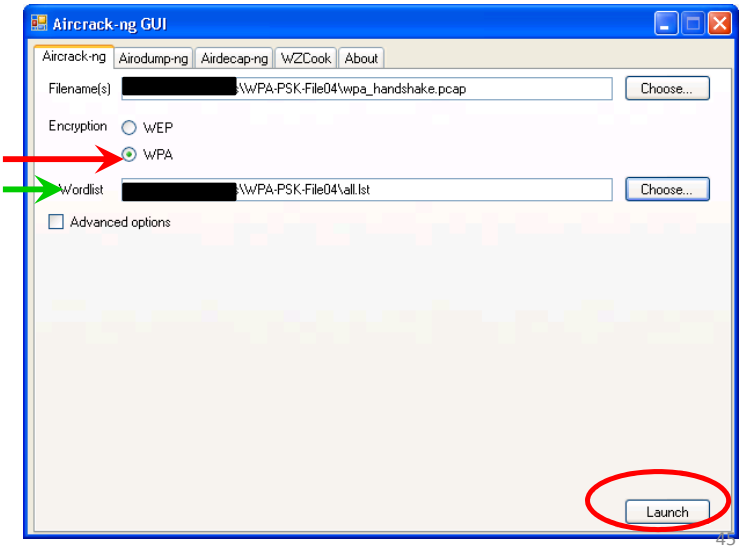
- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

Task ④: WPA-PSK Cracking

- The target wireless network is using WPA-PSK

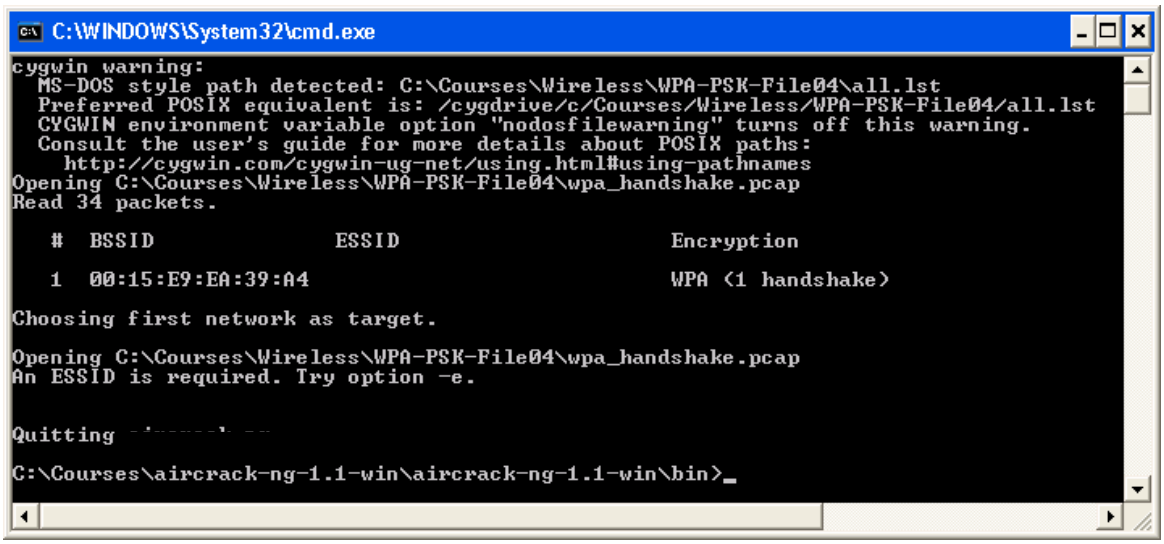
Task ④: WPA-PSK Cracking

- Filename(s) c:\wireless\wireless\WPA-PSK-File04\wpa_handshake.pcap
- Wordlist: c:\wireless\wireless\WPA-PSK-File04\all.lst



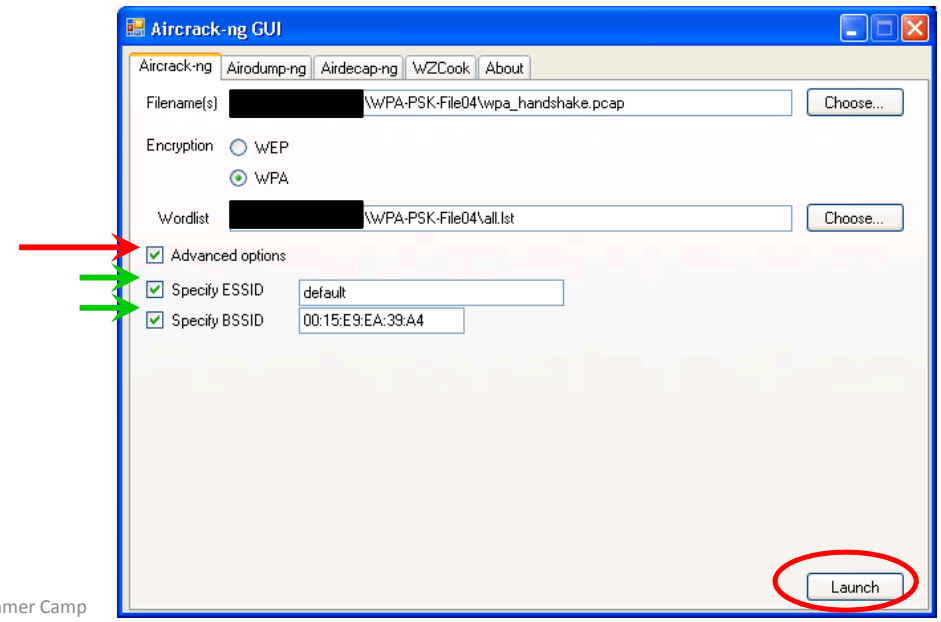
Task ④: What did you get?

- What?



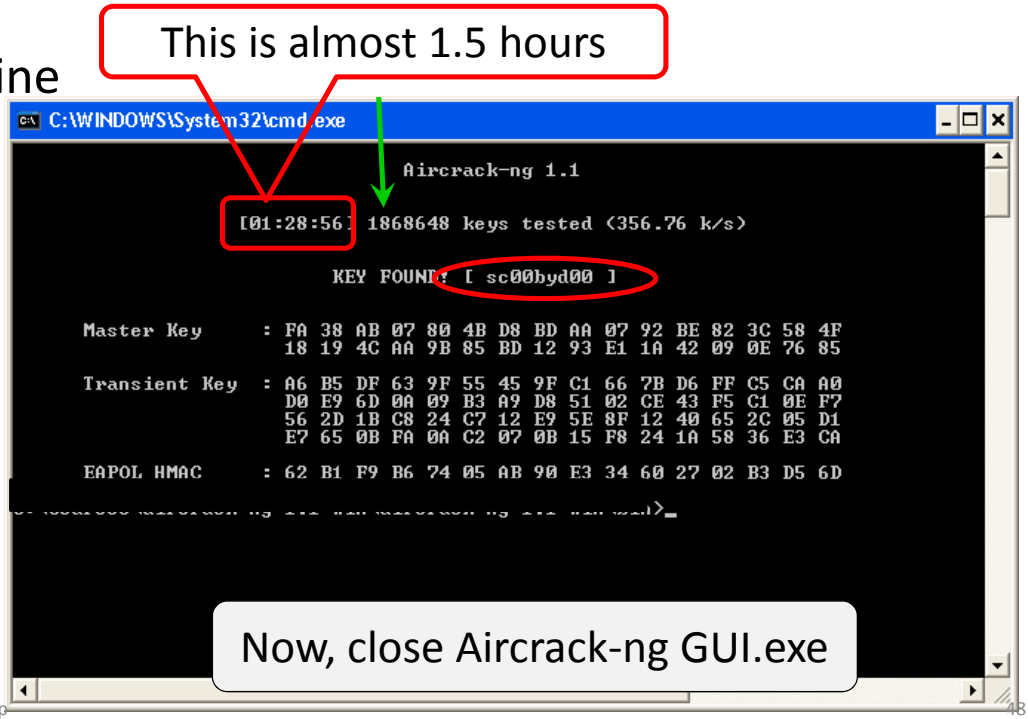
Task ④: WPA-PSK Cracking

- Advanced



Task ④: What did you get?

- Mine

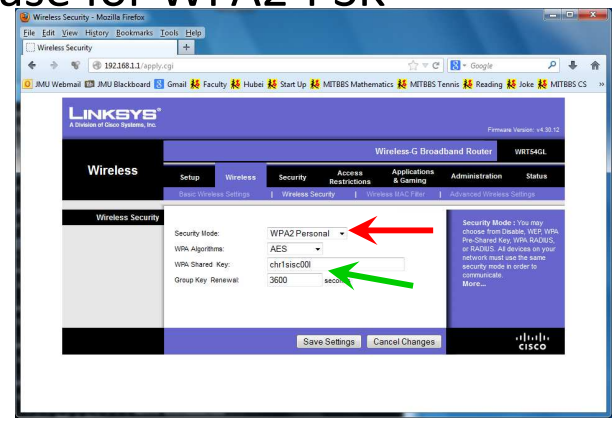


Now What?

- You can use the cracked WPA-PSK key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

Lesson to protect your wireless LAN?

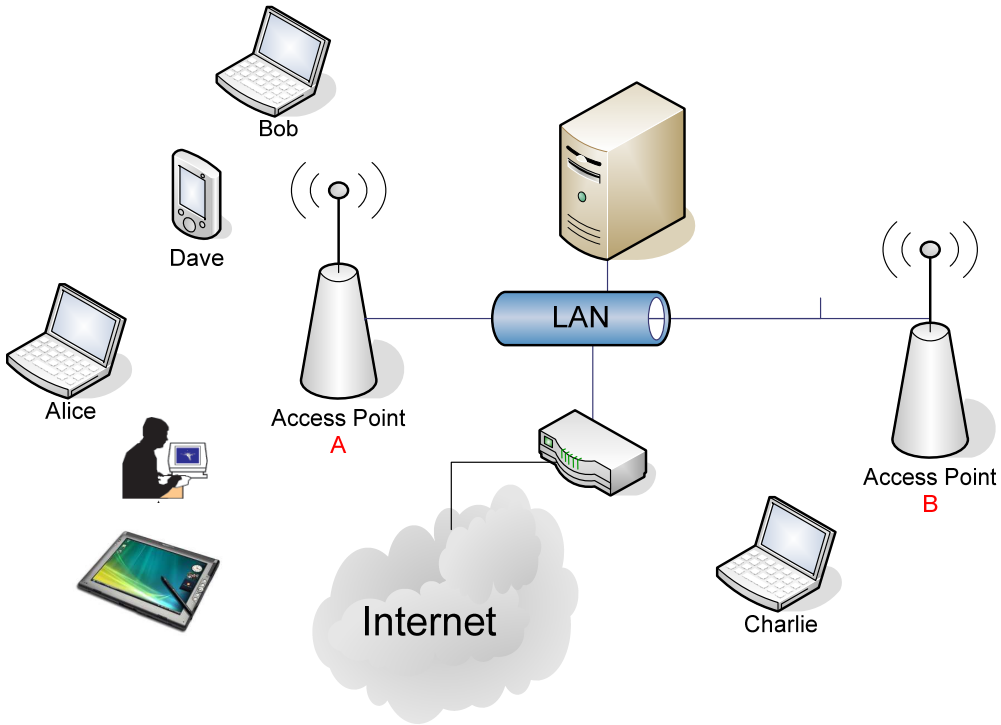
- Use WPA2 if you can
  - Definitely **no** WEP
  - Avoid WPA-PSK if you can
- Use a long passphrase for WPA2-PSK
  - ❖8 ~ 63 characters



Road Map

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2

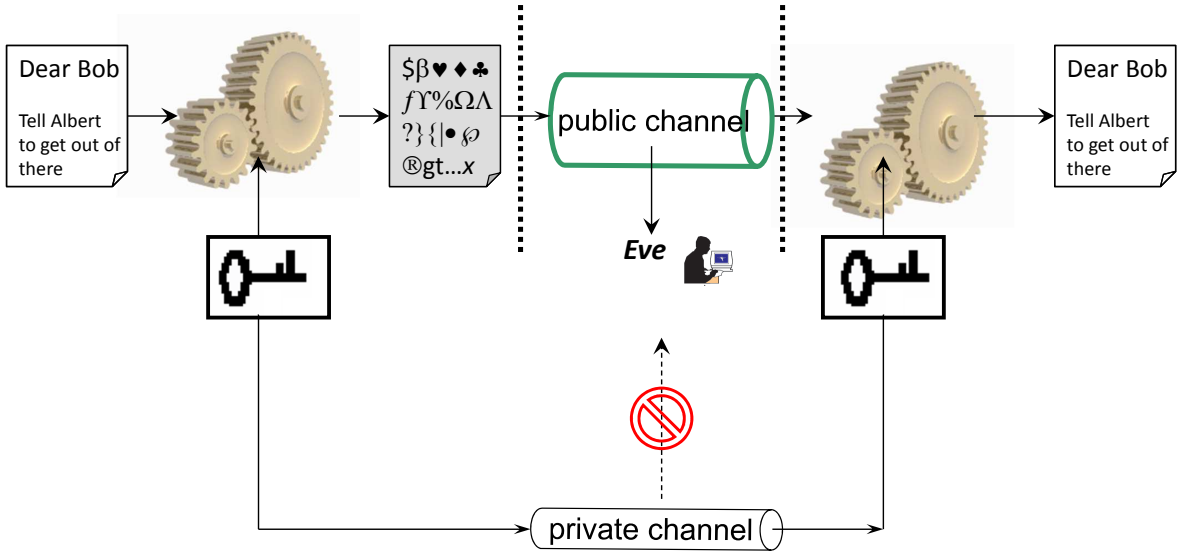
Wireless LAN Insecurity



Attacks Against Wireless LAN

- Hook to your wireless network and steal your data from your servers
- Eavesdrop on your wireless channel and steal passwords/secrets in transit

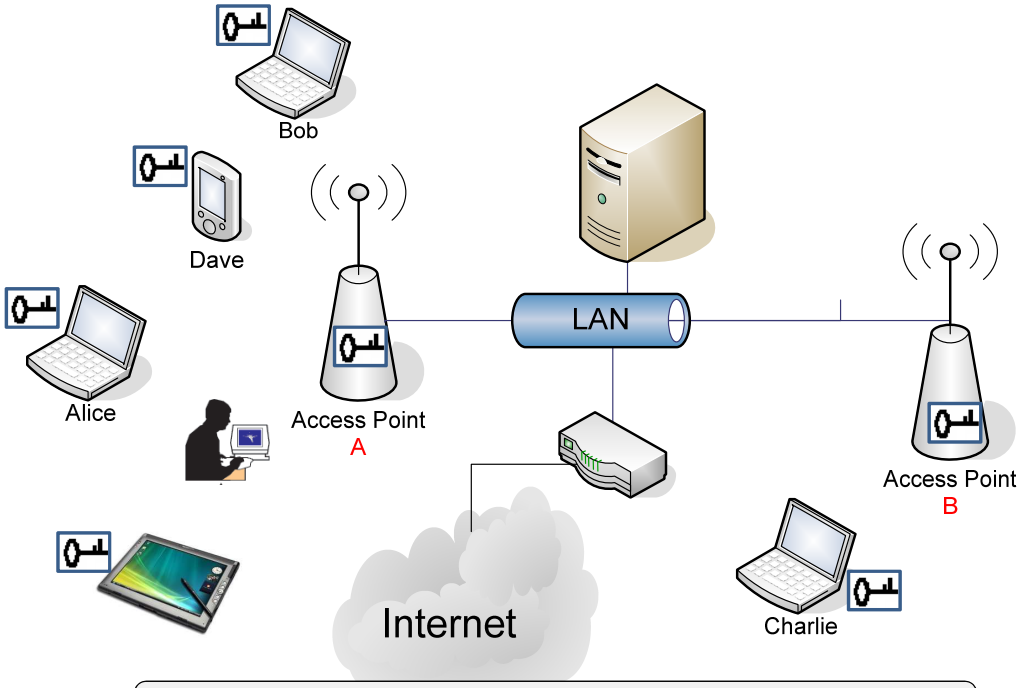
Symmetric Key Encryption



WEP

- Wired-equivalent privacy (WEP)
  - Security based on a shared secret (WEP key)
- Goals
  - Do not know the WEP key? No association or data transmission
  - Do not know the WEP key? No eavesdropping
  - Do not know the WEP key? No data injection
- Symmetric-key encryption algorithm: RC4
  - Implemented on
    - AP
    - Laptop: implemented by hardware

WEP: all users share the same key



A WEP key is either 40 bits or 104 bits

①WEP Configuration on AP

❶Wire your PC to your AP

– Your PC uses DHCP

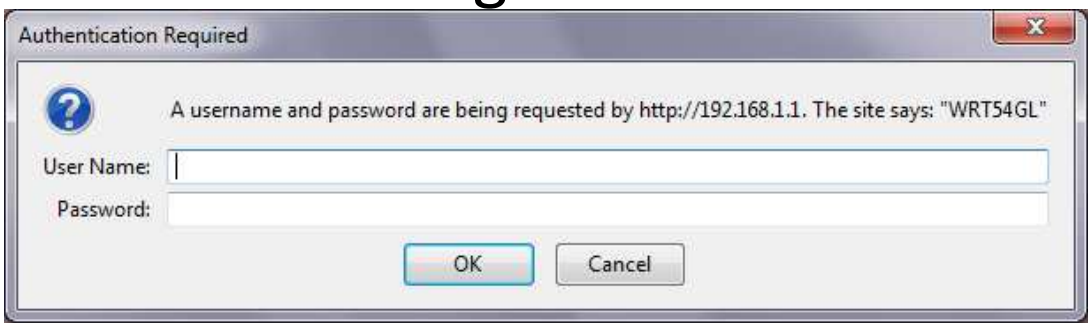
❷Check the IP address of your PC – ipconfig

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

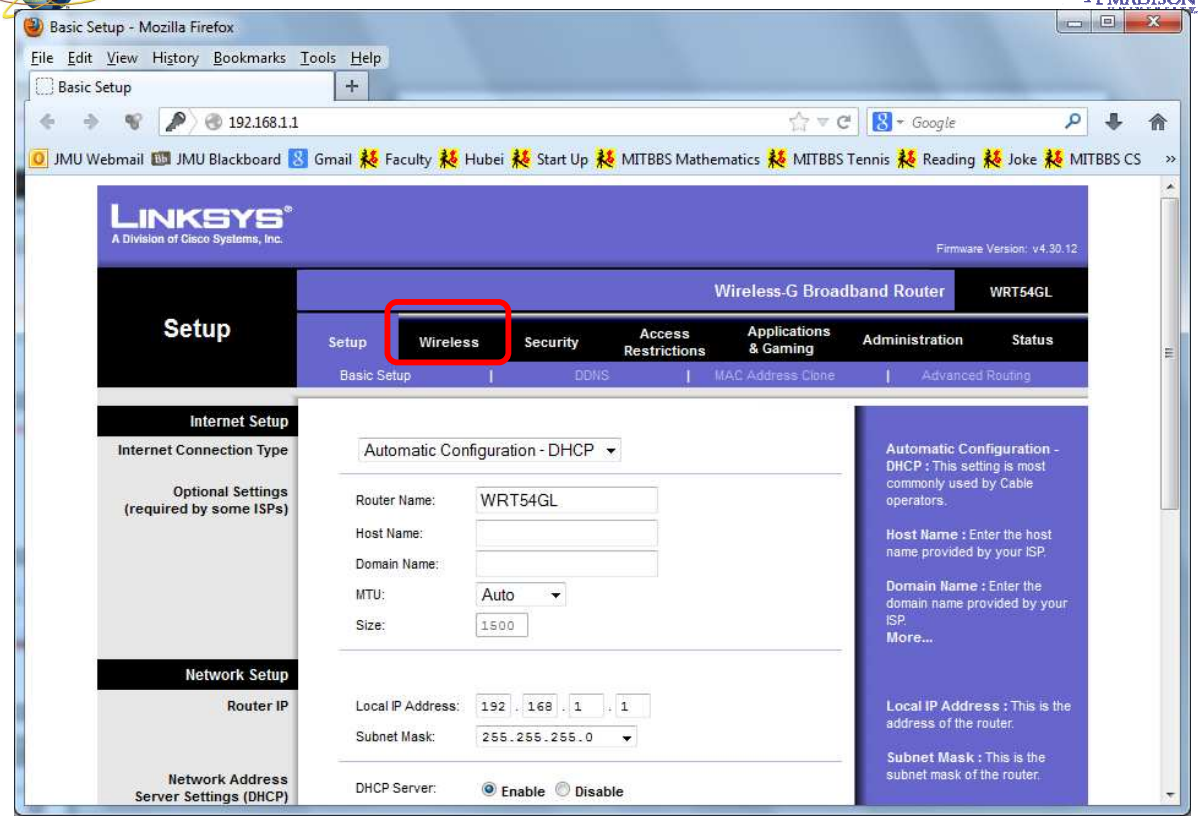
❸Open web browser, type in 192.168.1.1

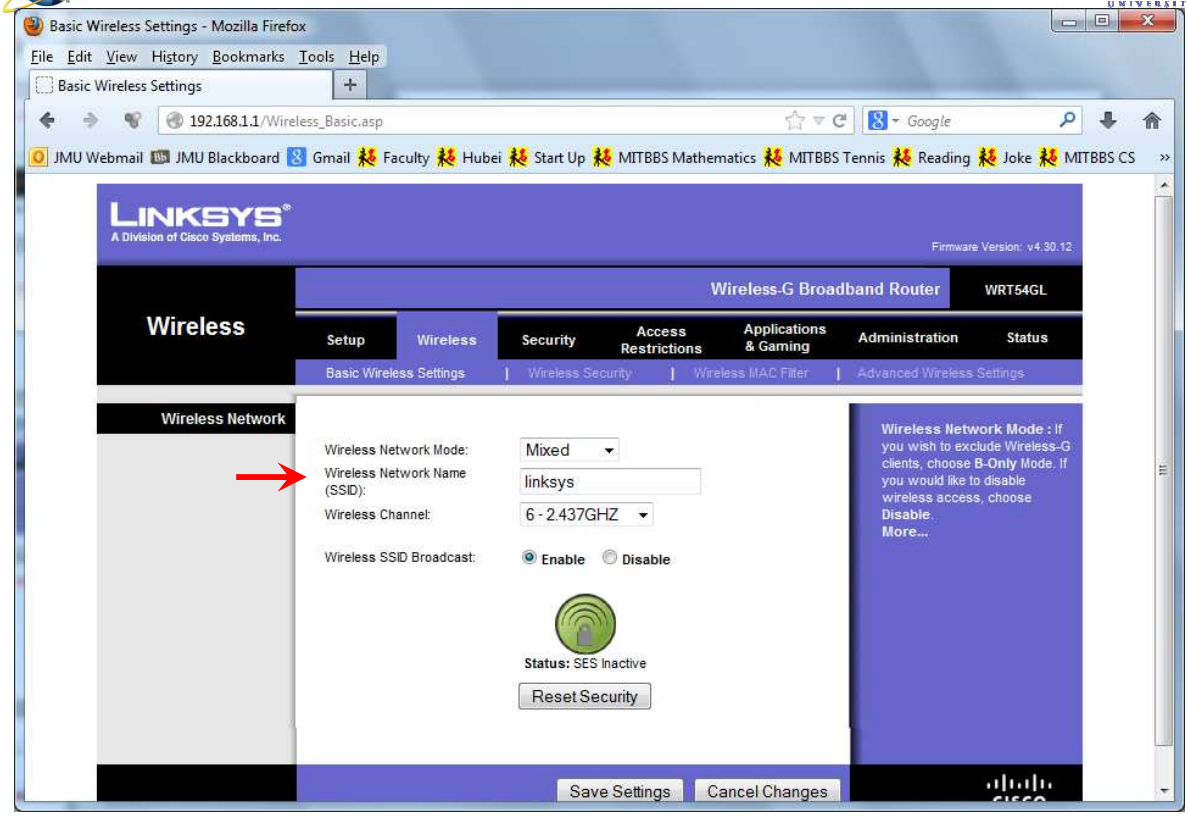
WEP Configuration on AP

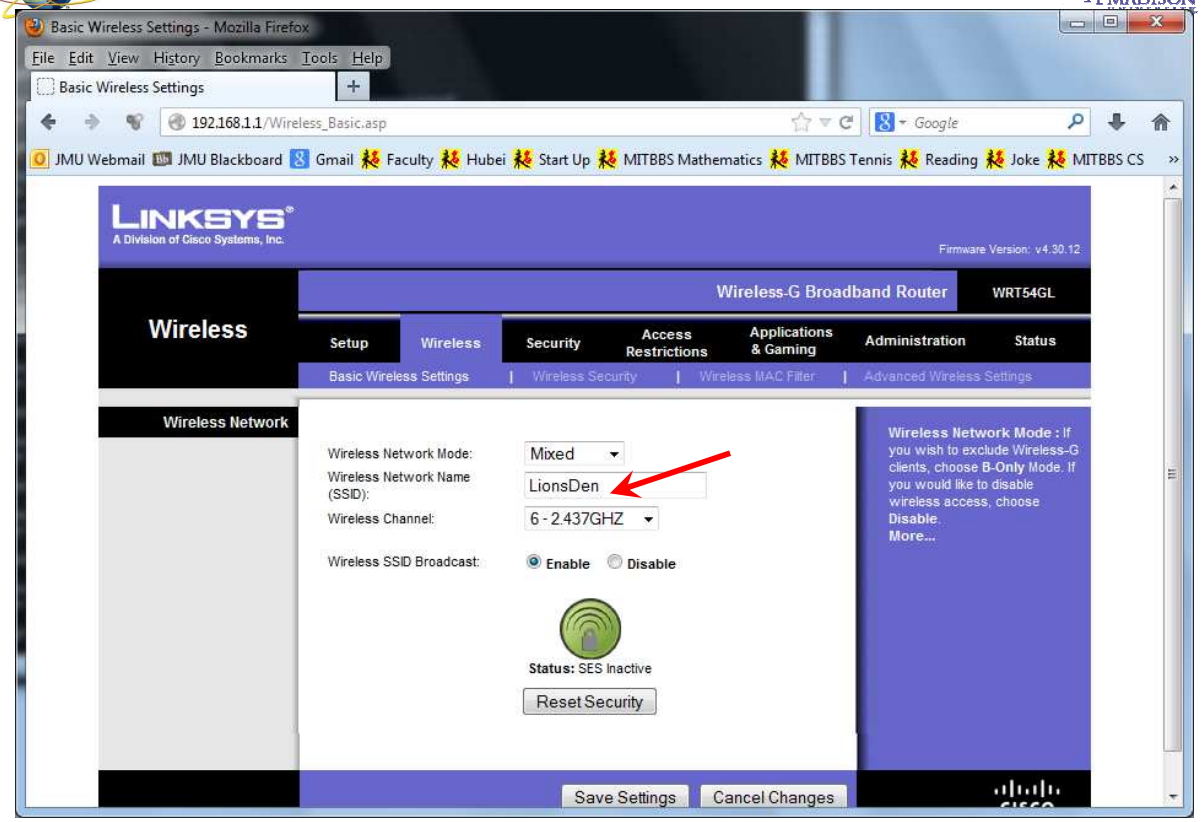


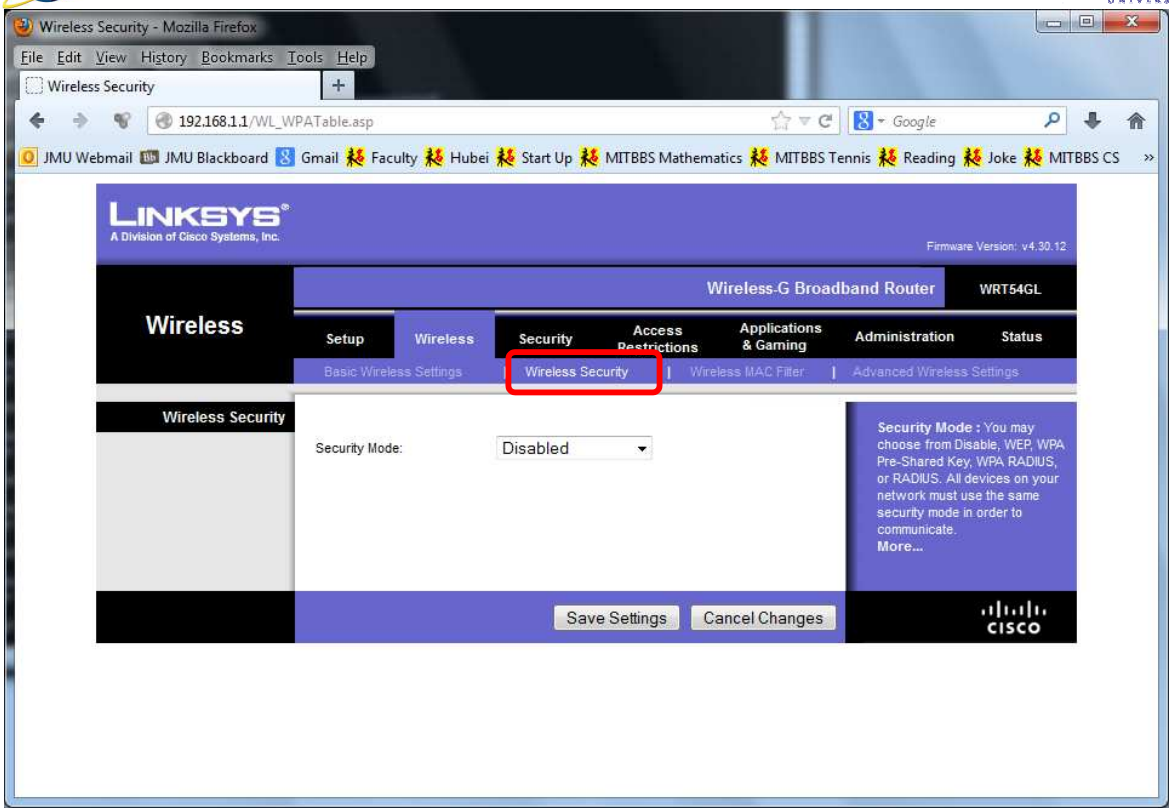
❹Use the default username and password

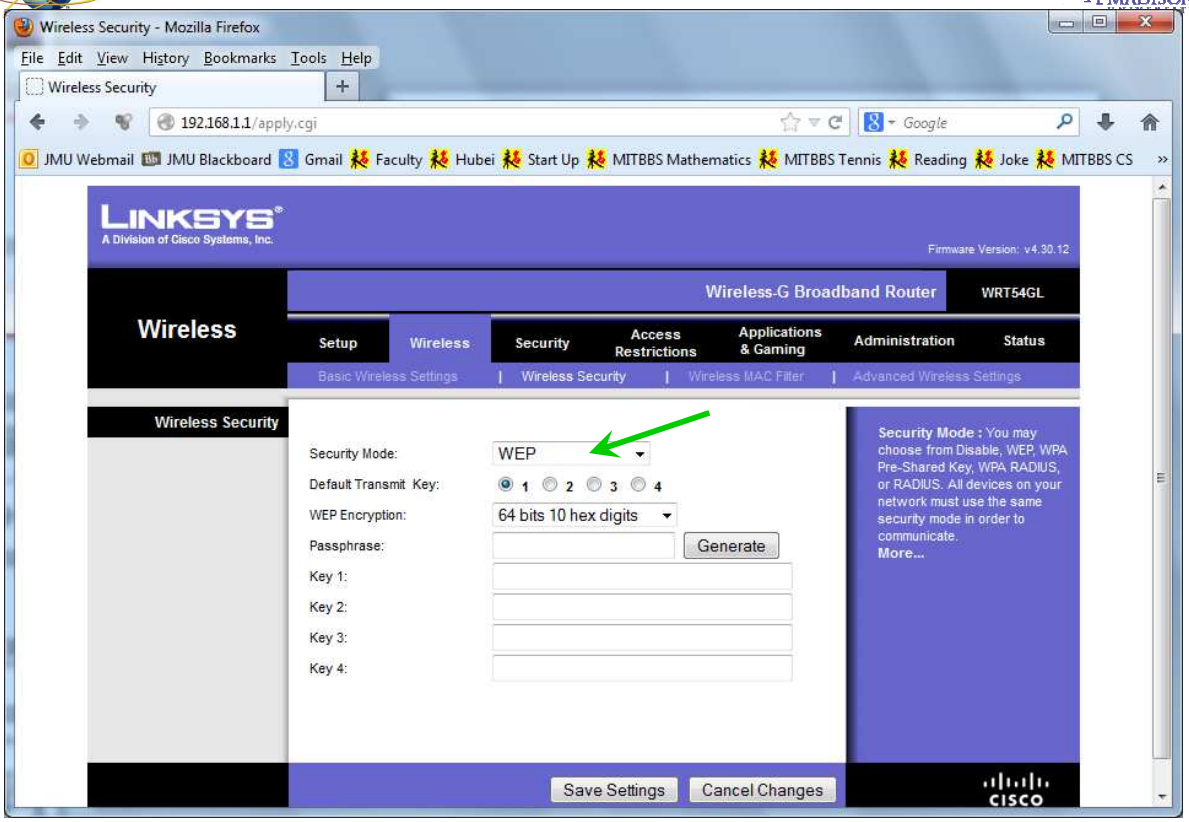
– For Linksys, it is admin/admin

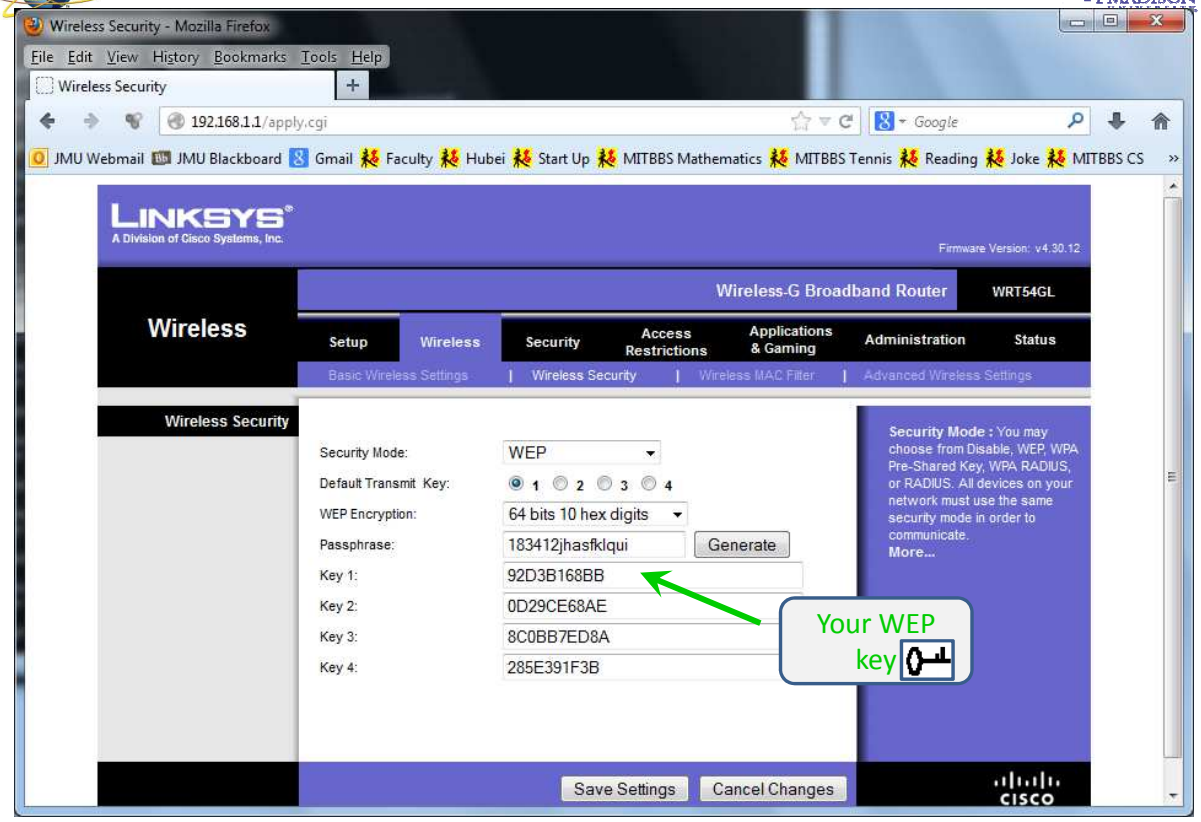

Basic Setup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Basic Setup
192.168.1.1
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router WRT54GL
Setup
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
Internet Setup
Internet Connection Type
Automatic Configuration - DHCP
Optional Settings (required by some ISPs)
Router Name: WRT54GL
Host Name:
Domain Name:
MTU: Auto
Size: 1500
Network Setup
Router IP
Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
Network Address Server Settings (DHCP)
DHCP Server: Enable Disable
Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.
Host Name : Enter the host name provided by your ISP.
Domain Name : Enter the domain name provided by your ISP.
More...
Local IP Address : This is the address of the router.
Subnet Mask : This is the subnet mask of the router.


Basic Wireless Settings - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Basic Wireless Settings
192.168.1.1/Wireless_Basic.asp
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router WRT54GL
Wireless
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Network
Wireless Network Mode: Mixed
Wireless Network Name (SSID): linksys
Wireless Channel: 6 - 2.437GHZ
Wireless SSID Broadcast: Enable Disable
Status: SES Inactive
Reset Security
Save Settings Cancel Changes
Wireless Network Mode : If you wish to exclude Wireless-G clients, choose B-Only Mode. If you would like to disable wireless access, choose Disable.
More...


Basic Wireless Settings - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Basic Wireless Settings
192.168.1.1/Wireless_Basic.asp
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router
WRT54GL
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Network
Wireless Network Mode: Mixed
Wireless Network Name (SSID): LionsDen
Wireless Channel: 6 - 2.437GHZ
Wireless SSID Broadcast: Enable Disable
Status: SES Inactive
Reset Security
Wireless Network Mode : If you wish to exclude Wireless-G clients, choose B-Only Mode. If you would like to disable wireless access, choose Disable.
More...
Save Settings
Cancel Changes


Wireless Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wireless Security
192.168.1.1/WL_WPATable.asp
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router
WRT54GL
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Security Mode: Disabled
Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...
Save Settings
Cancel Changes
cisco


Wireless Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wireless Security
192.168.1.1/apply.cgi
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router WRT54GL
Wireless
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Security Mode: WEP
Default Transmit Key: 1 2 3 4
WEP Encryption: 64 bits 10 hex digits
Passphrase: Generate
Key 1:
Key 2:
Key 3:
Key 4:
Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...
Save Settings Cancel Changes
cisco

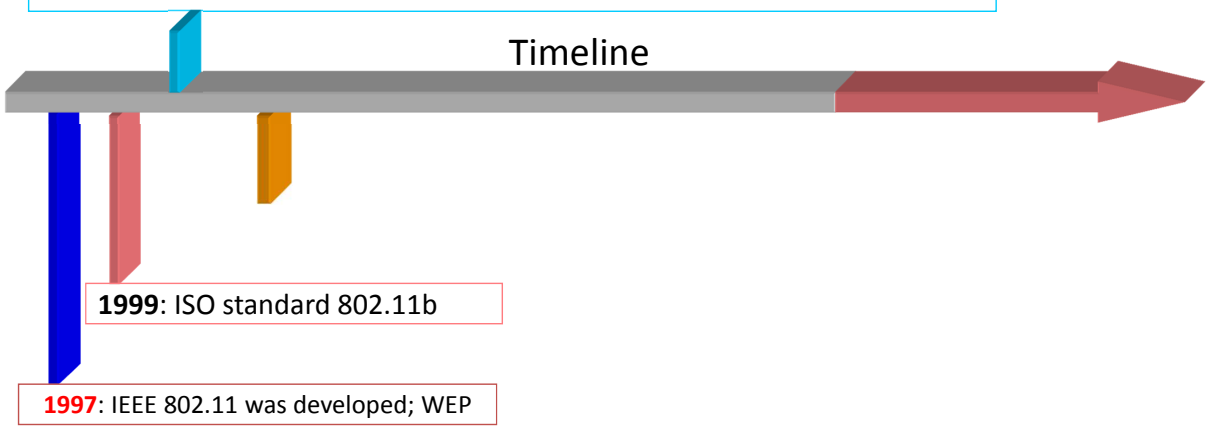

Wireless Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wireless Security
192.168.1.1/apply.cgi
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.12
Wireless-G Broadband Router WRT54GL
Wireless
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Security Mode: WEP
Default Transmit Key: 1 2 3 4
WEP Encryption: 64 bits 10 hex digits
Passphrase: 183412jhasfklqui Generate
Key 1: 92D3B168BB
Key 2: 0D29CE68AE
Key 3: 8C0BB7ED8A
Key 4: 285E391F3B
Your WEP key
Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...
Save Settings Cancel Changes
cisco

②WEP Configuration on Laptop

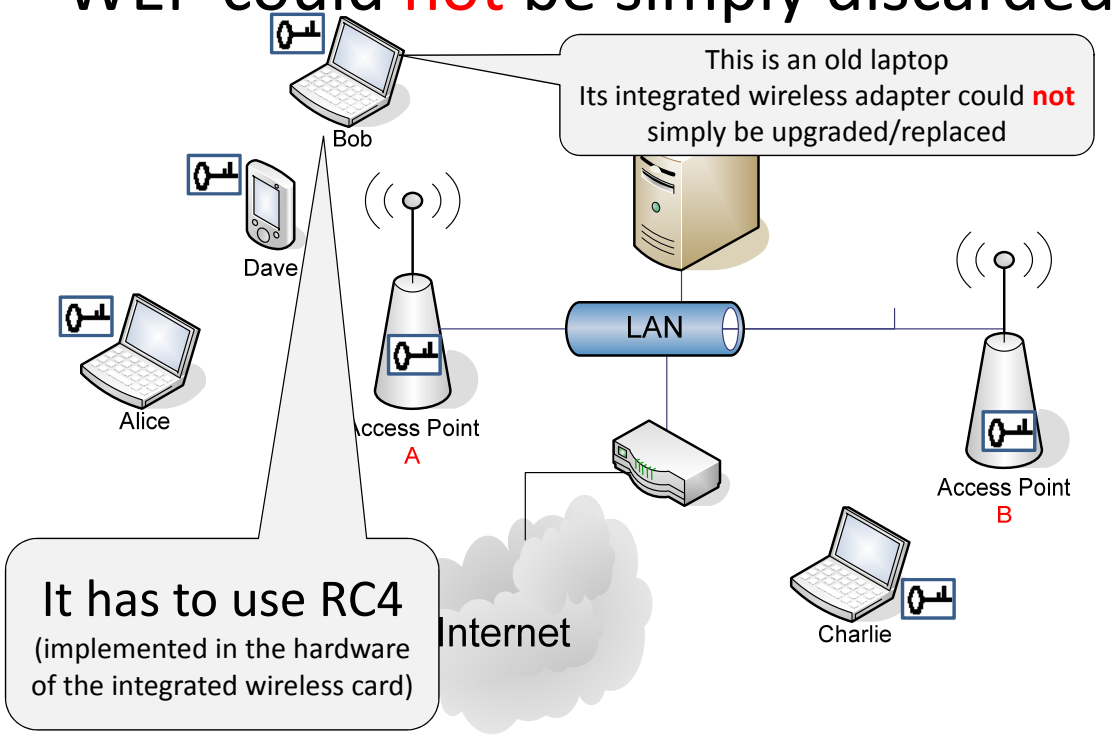
- Configure your laptop to connect to LionsDen
- With WEP key 92D3B168BB

WEP was Broken

2001
Borisov, Goldberg, Wagner [BGW01] discovered some practical flaws;
Arbaugh, Shanker, Wan [ASW01] also observed some flaws
Fluhrer, Mantin and Shamir [FMS01] found **fundamental** flaws
Stubblefield, Ioannidis and Rubin implemented the FMS01 attack
Rager released WEPCrack on August 12
Airsnort was released



WEP could not be simply discarded

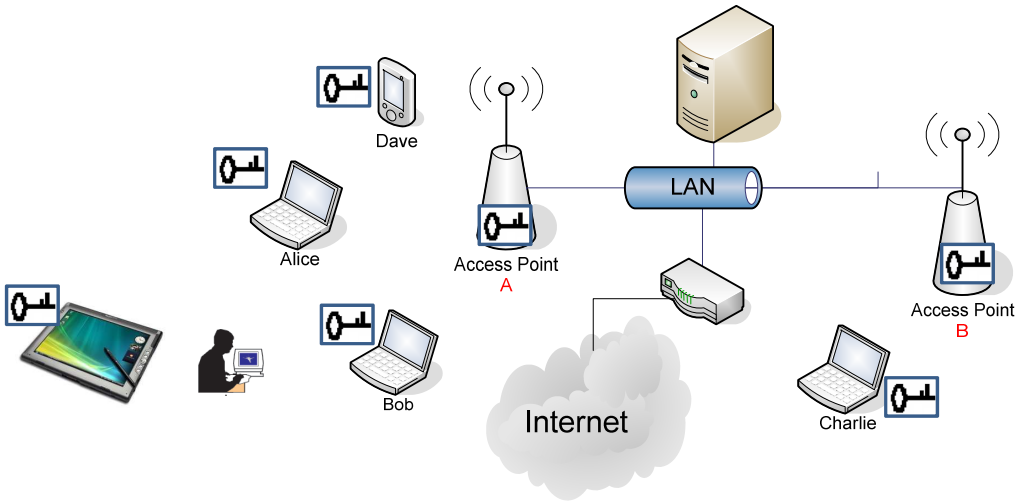


Short-term Fix: WPA

- Wifi-Protected Access (WPA)
  - Goal: **fix** WEP
  - Use the same encryption algorithm – RC4
- How?
  - Modify the way that packet encryption keys are generated

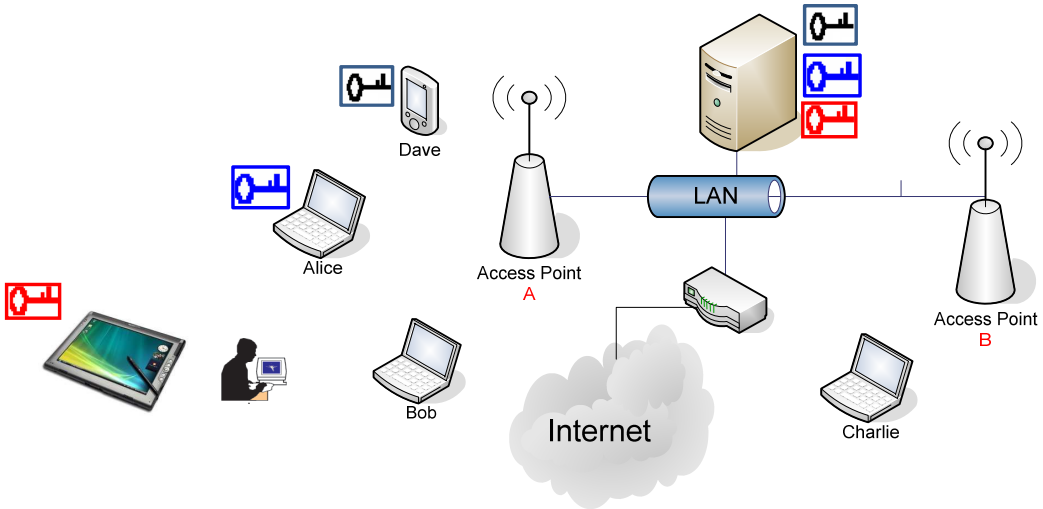
WPA Mode 1: WPA-PSK

- Pre-shared key (PSK)
- All users share the same passphrase



WPA Mode 2: WPA-Enterprise

- WPA-enterprise
- Each user has her/his own passphrase



①WPA-PSK Configuration on AP

❶Wire your PC to your AP

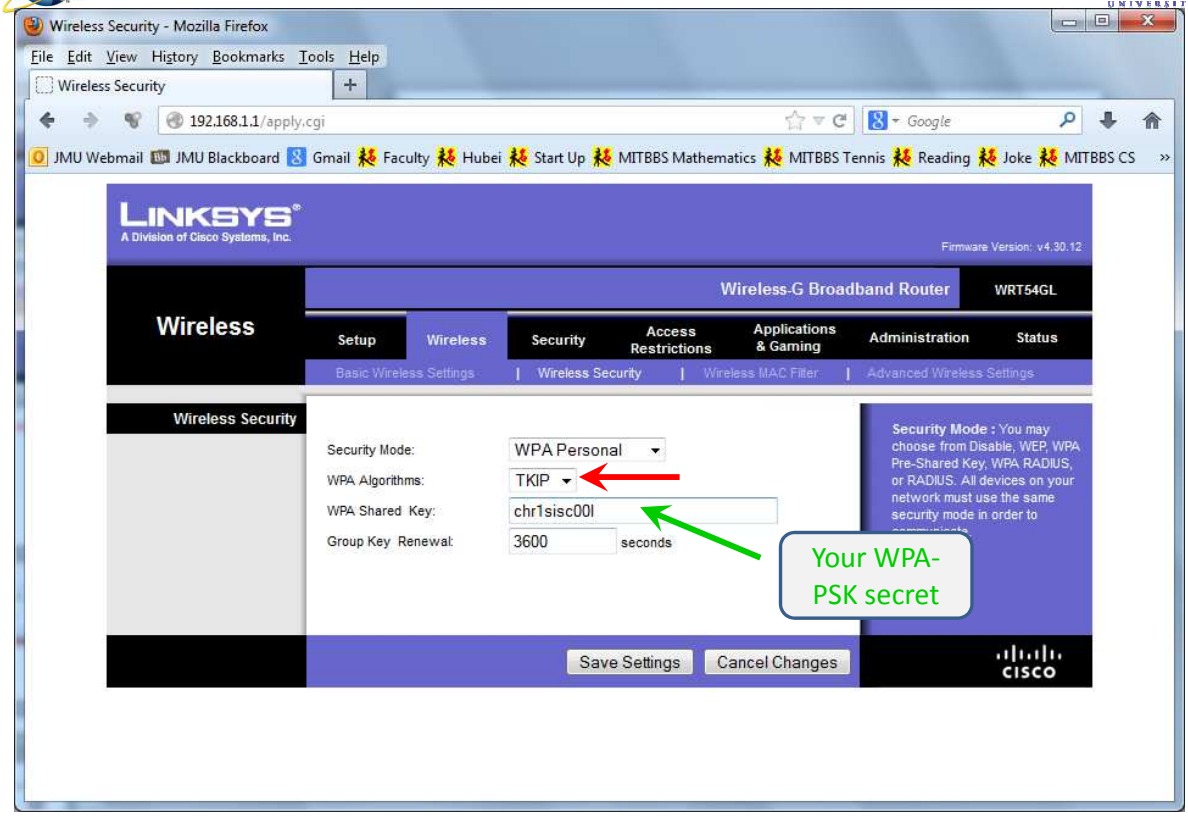
– Your PC uses DHCP

❷Check the IP address of your PC – ipconfig

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

❸Open web browser, type in 192.168.1.1



②WPA-PSK Configuration on Laptop

- Configure your laptop to connect to LionsDen
- With WPA-PSK secret chr1sisc00l

WPA-PSK is Weak Too!

- WPA's data integrity mechanism, Temporal Key Integrity Protocol (TKIP), is a temporary fix
  - It is vulnerable to more complex attacks
- WPA-PSK is based on shared secret
  - It may be susceptible to dictionary attacks and brute-force attacks

WPA2

- It uses a different encryption algorithm: Advanced Encryption Standard (AES)
  - More secure, standard
- It uses a more secure data integrity algorithm
  - CBC-MAC

⇒Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)

- Like WPA, WPA2 supports two modes
  - WPA2-PSK
  - WPA2-Enterprise

①WPA2-PSK Configuration on AP

❶Wire your PC to your AP

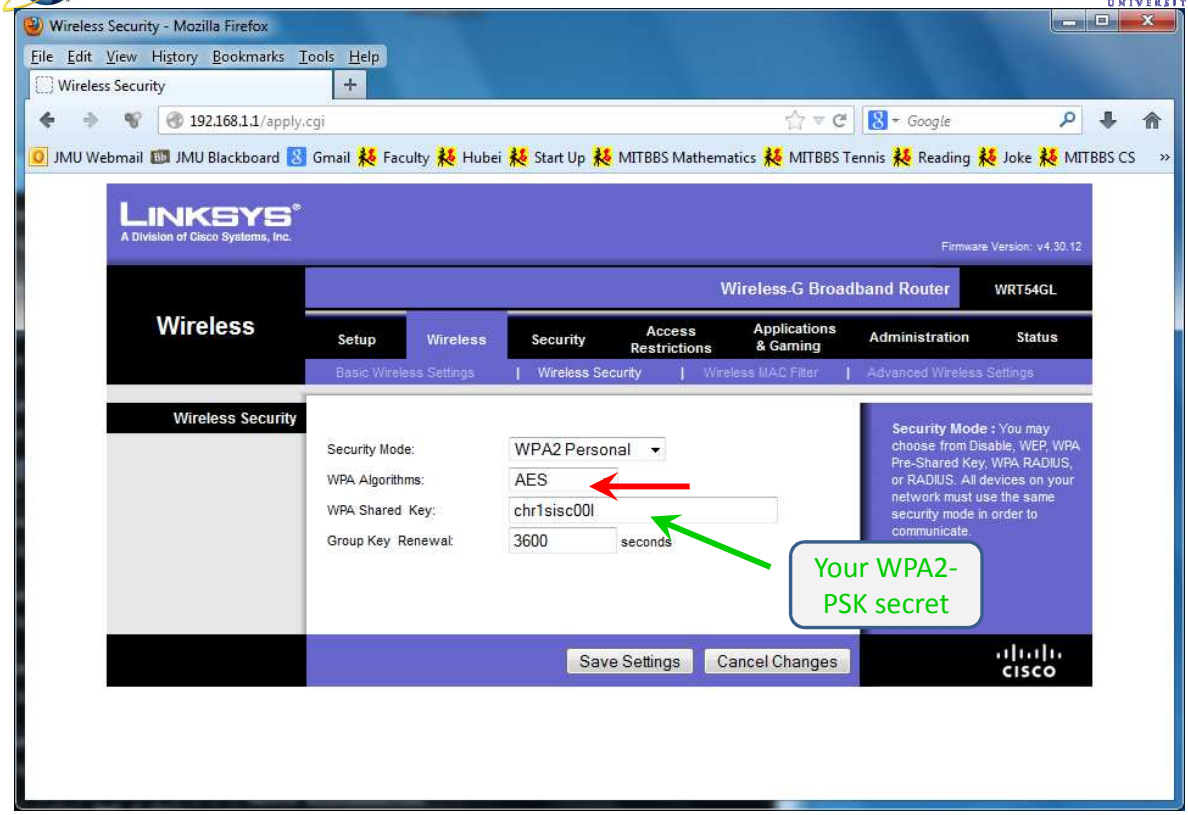
- Your PC uses DHCP

❷Check the IP address of your PC – ipconfig

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

❸Open web browser, type in 192.168.1.1

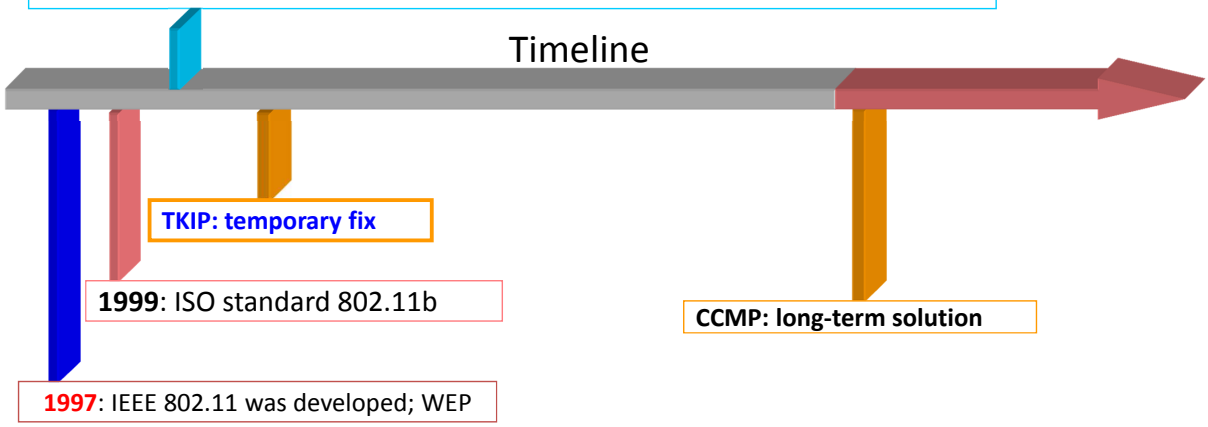


②WPA2-PSK Configuration on Laptop

- Configure your laptop to connect to LionsDen
- With WPA2-PSK secret chr1sisc00l

Wireless LAN Security: Summary

2001
Borisov, Goldberg, Wagner [BGW01] discovered some practical flaws;
Arbaugh, Shanker, Wan [ASW01] also observed some flaws
Fluhrer, Mantin and Shamir [FMS01] found **fundamental** flaws
Stubblefield, Ioannidis and Rubin implemented the FMS01 attack
Rager released WEPCrack on August 12
Airsnort was released



Buzzwords: Business vs. Technical

- WIFI
- Channel
- Wireless access point, wireless station (wireless cards)
- SSID
- ESSID
- WEP
- WPA
- WPA2
- Association/reassociate/dis associate

- RC4, TKIP, CCMP
  - AES, CTR, CBC-MAC
- 802.11
- 802.11i
- 802.11x
- MAC spoofing, MAC filtering
- Chipsets
- Managed mode
- Monitor mode

Summary

BUSINESS PEOPLE	ENCRYPTION	INTEGRITY	USER AUTHENTICATION	
		TKIP		

Summary

BUSINESS PEOPLE	ENCRYPTION	INTEGRITY	USER AUTHENTICATION	
WEP	RC4	Encrypted CRC	All users share the same key	
WPA-PSK	RC4	MIC	All users share the same key	
		TKIP		
WPA-Enterprise	RC4	MIC	Each user is separately authenticated	
WPA2-PSK	AES-CTR	(CBC-MAC)	All users share the same key	home
WPA2-Enterprise	AES-CTR	(CBC-MAC)	Each user is separately authenticated	

How to Find Target AP's MAC

- Need a computer with wireless support
- On Windows
  - Netstumbler: freeware; http://www.netstumbler.com/downloads/
- On Linux
  - ifconfig wlan0 down
  - iwconfig wlan0 mode managed
  - sudo iwlist **wlan0** scan

Summary

- Exercises
  - ①Cracking captured WEP traffic 1
  - ②Crack captured WPA-PSK traffic 2
  - ③Cracking captured WEP traffic 3
  - ④Crack captured WPA-PSK traffic 4
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2