

Foundations of Network and Computer Security

John Black

Lecture #23
Nov 16th 2004

CSCI 6268/TLEN 5831, Fall 2004

Announcements

- Proj #2 – Due next class
 - Distance students may email their project to Mazdak
- Proj #3 – Due Dec 2nd
 - Start now if you haven't already!
- Reading: WEP paper (on our website)
- Quiz #4: a week from today

Phishing Revisited

Dear Amazon User,

During our regular update and verification of the accounts, we could not verify your current information. Either your information has changed or it is incomplete.

As a result, your access to buy on Amazon has been restricted. To continue using your Amazon account again, please update and verify your information by clicking the link below :

**[http://www.amazon.com@service02.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0
&pUserId=&us=445&ap=0&dz=1&Lis=10&ref=br_bx_c_2_2](http://www.amazon.com@service02.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0&pUserId=&us=445&ap=0&dz=1&Lis=10&ref=br_bx_c_2_2)**

Thank you very much for your cooperation!
Amazon Customer Support

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Amazon.com
Earth's Biggest Selection


Amazon.com Sign In - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Back Forward Stop Home Search Favorites Media Print Mail AutoFill

Address: http://service02.com/exec/jobidos/subst/home/?EnterConfirm&UsingSSL=0&pUserId=&us=445&ap=0&dz=1&Lis=10&ref=br_bx_c_2_2

Google Search Web PageRank 741 blocked AutoFill

amazon.com  [VIEW CART](#) | [WISH LIST](#) | [YOUR ACCOUNT](#) | [HELP](#)

[WELCOME](#) | [YOUR STORE](#) | [BOOKS](#) | [APPAREL & ACCESSORIES](#) | [ELECTRONICS](#) | [TOYS & GAMES](#) | [MUSIC](#) | [MAGAZINE SUBSCRIPTIONS](#) | [SEE MORE STORES](#)

 **Your Gold Box**

What is your e-mail address?

My e-mail address is

Do you have an Amazon.com password?

No, I am a new customer.

Yes, I have a password:

[Sign in using our secure server](#)

- [Forgot your password? Click here](#)

- [Has your e-mail address changed since your last order?](#)

The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our [standard server](#).

[Top of Page](#)

[Amazon.com Home](#) | [Directory of All Stores](#)

Our International Sites: [Canada](#) | [United Kingdom](#) | [Germany](#) | [Japan](#) | [France](#)

[Contact Us](#) | [Help](#) | [Shopping Cart](#) | [Your Account](#) | [Sell Items](#) | [1-Click Settings](#)

[Investor Relations](#) | [Press Releases](#) | [Join Our Staff](#)

[Conditions of Use](#) | [Privacy Notice](#) © 1996-2004, Amazon.com, Inc. or its affiliates

Internet

Where does the info go?

- service02.com maps to IP 66.218.79.155

```
% whois 66.218.79.155
```

```
OrgName:      Yahoo!
```

```
OrgID:        YA00
```

```
Address:      701 First Avenue
```

```
City:         Sunnyvale
```

```
StateProv:    CA
```

```
NetRange:     66.218.64.0 - 66.218.95.255
```

Wireless Security

- Why is wireless security essentially different from wired security?
 - Almost impossible to achieve physical security on the network
 - Slot machine example
 - You can no longer assume that restricting access to a building restricts access to a network
 - The “parking lot attack”

Wireless Security Challenges

- Further challenges:
 - Many wireless devices are resource-constrained
 - Laptops are pretty powerful these days but PDAs are not
 - Sensors are even more constrained
 - RFIDs are ridiculously constrained
 - Paradox: the more resource-constrained we get, the more ambitious our security goals tend to get



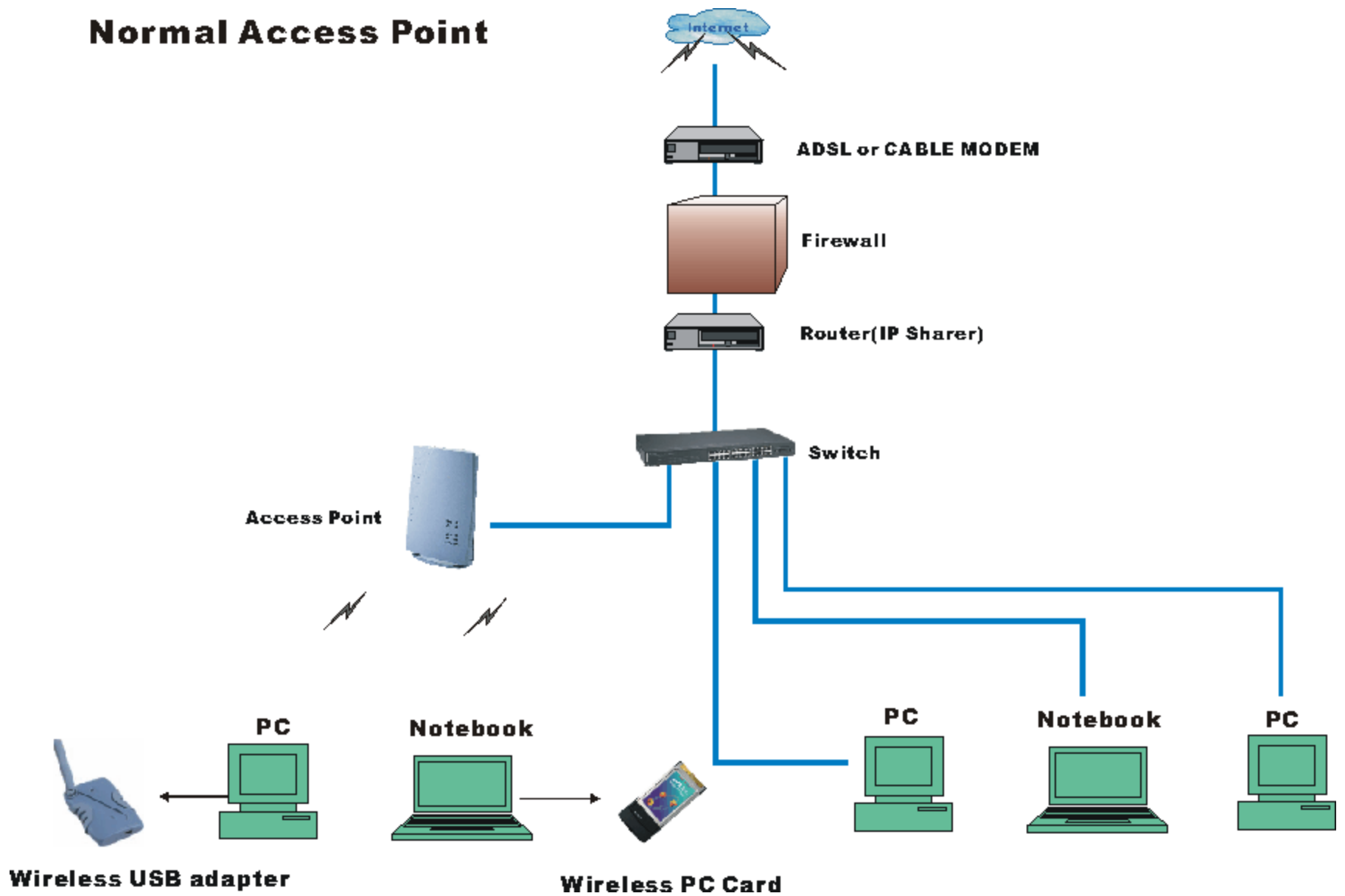
IEEE 802.11a/b/g

- A standard ratified by IEEE and the most widely-used in the world
 - Ok, PCS might be a close contender
 - Also called “Wi-Fi”
 - 802.11 products certified by WECA (Wireless Ethernet Compatibility Alliance)
 - Bluetooth is fairly commonplace but not really used for LANs
 - More for PANs (the size of a cubicle)
 - Connect PDA to Cell Phone to MP3, etc.

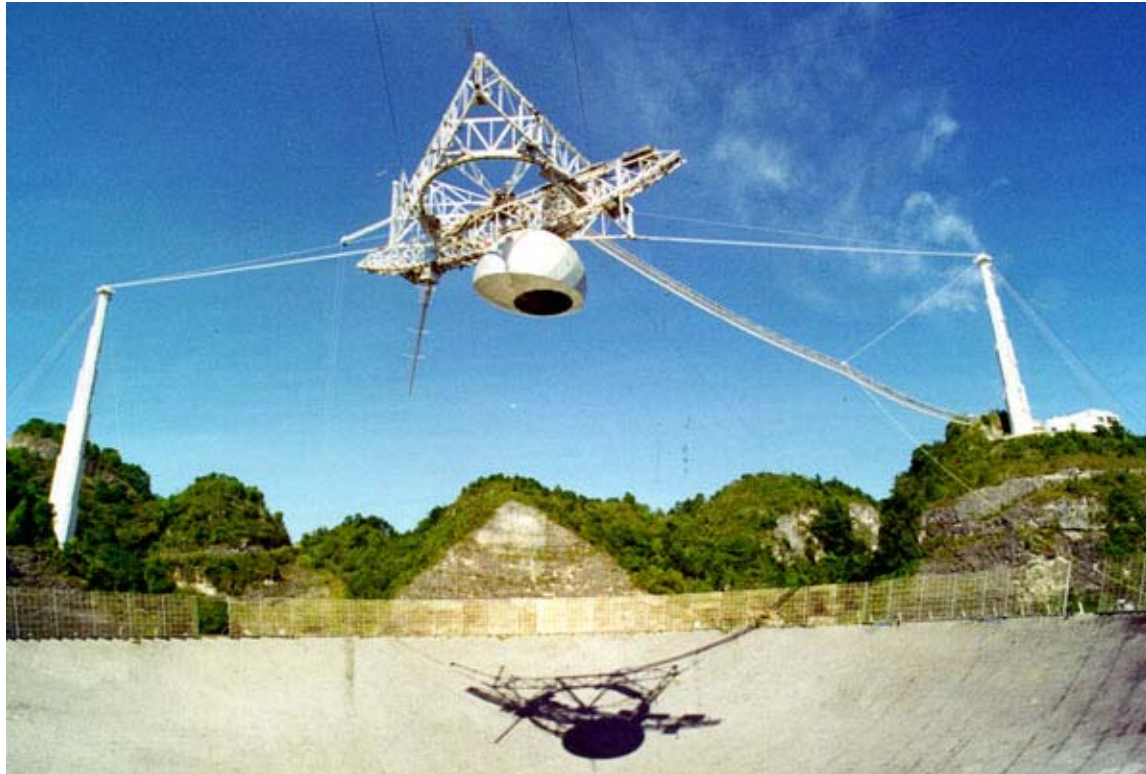
Wireless Network Architecture

- Ad Hoc
 - Several computers form a LAN
- Infrastructure
 - An access point (AP) acts as a gateway for wireless clients
 - This is the model we're most used to
 - Available all through the EC, for example
 - Mark's probably in the back using one right now

Normal Access Point



My Access Point

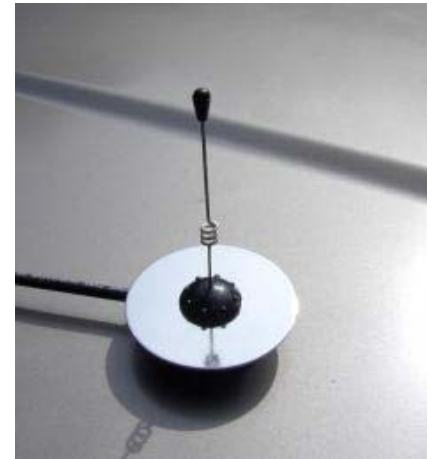


War Driving

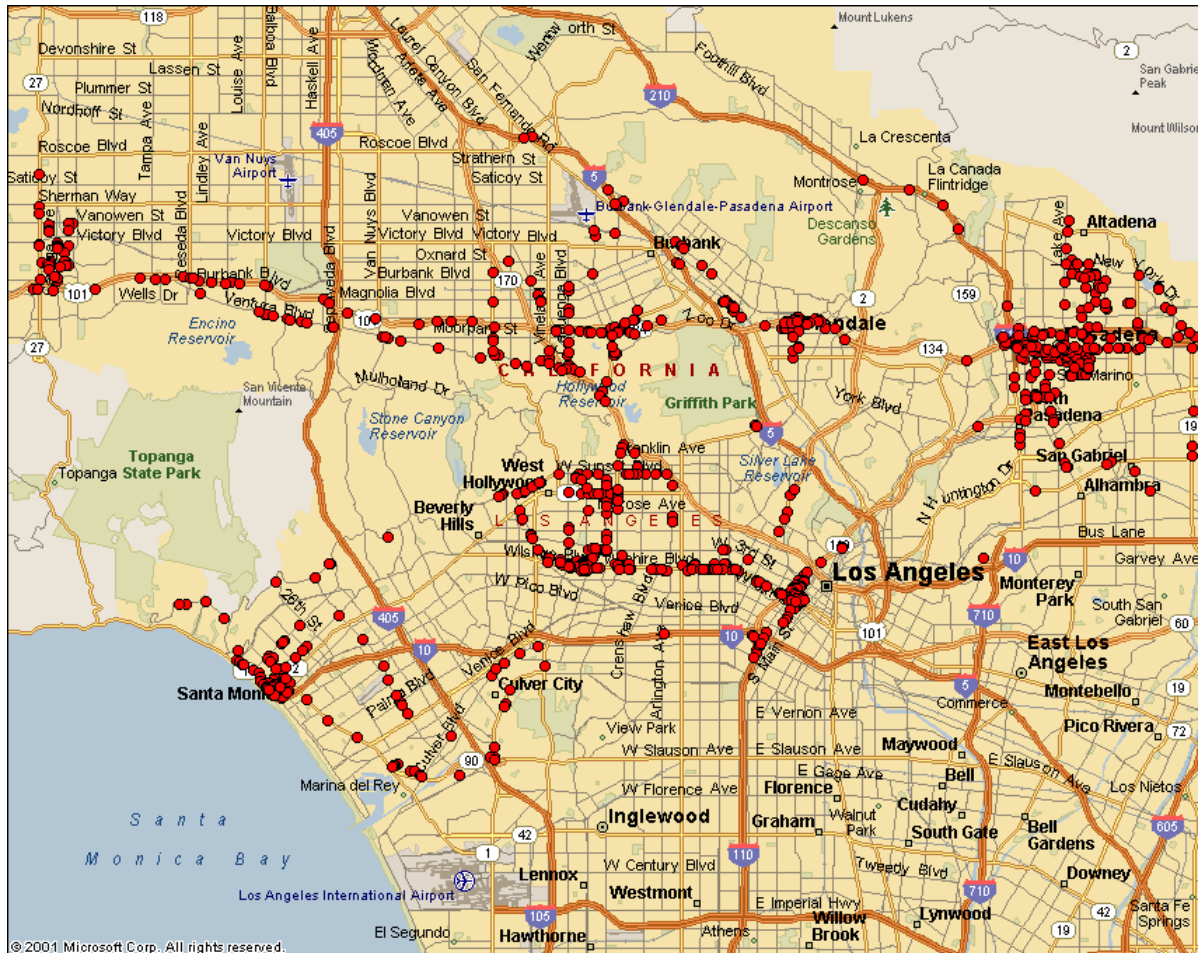
- The inherent physical insecurity of wireless networks has led to the “sport” of war-driving
 - Get in your car, drive around, look for open access points with you laptop
 - Name comes from the movie “War Games”
 - Some people get obsessed with this stuff
 - You can buy “war driving kits” on line
 - Special antennas, GPS units to hook to you laptop, mapping software

More War Driving

- People use special antennas on their cars
 - It used to be Pringles cans, but we've moved up in the world
- People distribute AP maps
- War driving contest at BlackHat each year



Next Time You're in LA



What's the Big Deal?

- My home access point is wide-open
 - People could steal bandwidth
 - I'm not that worried about it
 - People could see what I'm doing
 - I'm not that worried about it
- There are ways to lock-down your access point
 - MAC filtering
 - Non-signalling APs and non-default SSIDs
 - Wired Equivalent Privacy (WEP)

MAC Filtering

- Allow only certain MACs to associate
 - Idea: you must get permission before joining the LAN
 - Pain: doesn't scale well, but for home users not a big deal
 - Drawback: people can sniff traffic, figure out what MACs are being used on your AP, then spoof their MAC address to get on

Non-Signalling APs

- 802.11 APs typically send a “beacon” advertising their existence (and some other stuff)
 - Without this, you don’t know they’re there
 - Can be turned off
 - If SSID is default, war drivers might find you anyway
 - SSID is the “name” of the LAN
 - Defaults are “LinkSYS”, NETGEAR, D-Link, etc
 - Savvy people change the SSID and turn off beacons
 - SSID’s can still be sniffed when the LAN is active however, so once again doesn’t help much

Let's Use Crypto!

- WEP (Wired Equivalent Privacy)
 - A modern study in how not to do things
 - The good news: it provides a wonderful pedagogical example for us
- A familiar theme:
 - WEP was designed by non-cryptographers who knew the basics only
 - That's enough to blow it

WEP Protocol

- One shared key k , per LAN
 - All clients and APs have a copy of k
 - We are therefore in the symmetric key setting
 - Very convenient: no public key complexities needed
 - Has drawbacks, as we'll see later
 - In the symmetric key model, what do we do (minimally) for data security?
 - Authentication and Privacy!
 - (MAC and encrypt)

WEP Protocol

- For message M , $P = (M, c(M))$
 - $c()$ is an *unkeyed* CRC (cyclic redundancy check)
- Compute $C = P \oplus \text{RC4}(v, k)$
 - RC4 is a stream cipher
 - Think of a stream cipher as a “randomness stretcher”: give it n random bits and it produces (essentially) infinite pseudo-random bits
 - The input is variously called the “seed” or the “key”
 - Seems a lot like a pseudo-random number generator!
 - We will look at RC4 in more detail later
 - v is an IV
 - As usual, the IV should never be repeated over the life of the key
- Sender transmits (v, C)

WEP Decryption

- Receiver obtains (v', C') and knows k
 - Computes $C' \oplus RC4(v', k) = (P' \oplus RC4(v', k)) \oplus RC4(v', k) = P'$
 - Then checks integrity with $P' = (M', c')$ and asking whether $c' = c(M')$
 - If not, reject the frame as inauthentic
 - Looks familiar, but we should be suspicious: a keyless function is *not* a MAC!

Goals

- Security Goals of WEP:
 - Privacy
 - Integrity
 - What we also have called “authenticity”
 - It should be “hard” to tamper with ciphertexts without being detected
 - It should be “hard” to forge packets
 - Access Control
 - Discard all packets not properly encrypted with WEP (optional part of the 802.11 standard)
- WEP Document:
 - Security “relies on the difficult of discovering the secret key through a brute-force attack”

WEP Keys

- 802.11 was drafted when 40 bits were all we could export
 - This restriction was lifted in 1998, but the standard was already in draft form
 - Some manufacturers extended the key to an optional 128-bit form
 - This is misleading: the 128 form uses a 104 bit key because the IV is 24 bits

WEP Keys

- Two forms: the 40 bit key

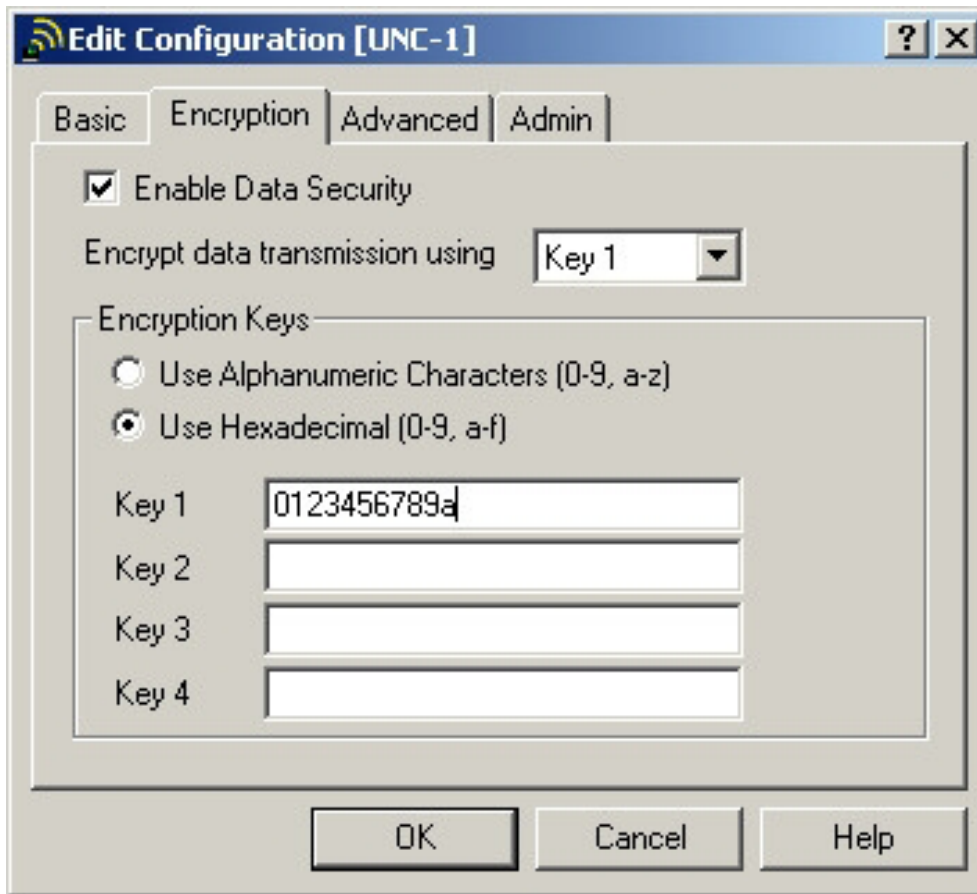


- The “128” bit key



Recall: IV is public, so shouldn't count as “key”

Entering WEP Keys



Note: Four keys allowed to encourage key-rotation, but this has to all be synchronized among all users of the WLAN.

Goals Achieved: \emptyset

- Let's start with the Privacy goal
 - WEP is using an encryption pad; what is the cardinal rule of encryption pads?
 - So how might a pad be re-used?
 - If the IV repeats, the pad will repeat:
 - Pad is $RC4(v, k)$
 - k is fixed for all communications
 - Since IV is public, an attack sees when the IV repeats

IV repeats

- It's bad:
 - Some cards fix IV=0, end of story
 - (This is 802.11 compliant, by the way!)
 - Some cards re-initialize IV to 0 each time they are powered up
 - So each time you insert a PCMCIA card into your laptop, or power up your laptop
 - IV repeats in the lower range far more likely here
 - The IV is only 24 bits, so eventually it will wrap around
 - 1500-byte packets, 5Mbps, IV wraps in less than 12 hours
 - With random IVs, the birthday effect says we expect a repeat within 5000 packets (a few mins in the scenario above)

What to do with repeated IVs?

- Build a “decryption dictionary”
 - Once we figure out the plaintext
 - Because it’s broadcast in the clear and encrypted
 - Because it’s part of a standard transmission
 - Because you injected the message from the outside
 - ...then we know the keystream
 - Put keystream and IV into a table for later use
 - Allows quick decryption of any ciphertext where we know the keystream of its IV
 - About 24 GB to store 1500 bytes for each of the possible 2^{24} IVs
- Note: it would probably be easier to brute-force the 40-bit key
 - But this approach works against the 104-bit key as well

Authentication

- Recall $c()$ was a CRC
 - CRC's are polynomials over a Galois Field of characteristic 2; therefore they are linear over addition, which in this field is \oplus
 - Hunh?
 - Function c has the following property:
 - $c(x \oplus y) = c(x) \oplus c(y)$
 - This property lets us modify any ciphertext such that the WEP integrity check will still pass
 - $C = RC4(v, k) \oplus (M, c(M))$
 - We want to change M to M'

Altering WEP Ciphertext

- Suppose we want $M' = M \oplus \Delta$ instead of M
 - Compute $C' = C \oplus (\Delta, c(\Delta))$
 - Let's check:
 - $C' = C \oplus (\Delta, c(\Delta))$
 - $= \text{RC4}(v, k) \oplus (M, c(M)) \oplus (\Delta, c(\Delta))$
 - $= \text{RC4}(v, k) \oplus (M \oplus \Delta, c(M) \oplus c(\Delta))$
 - $= \text{RC4}(v, k) \oplus (M', c(M \oplus \Delta))$
 - $= \text{RC4}(v, k) \oplus (M', c(M'))$
 - Note: we don't need to know what M is to do this; we can blindly modify M as we desire

Defeating the WEP Access Mechanism

- Recall that mal-formed WEP packets are discarded (optional feature)
 - If we know *one* plaintext and its corresponding ciphertext, we are able to inject arbitrary traffic into the network
 - Suppose we know M , v , and $C = RC4(v, k) \oplus (M, c(M))$
 - Then we know $c(M)$ // $c()$ is public and unkeyed
 - So we know $RC4(v, k)$
 - Now we can produce $C' = RC4(v, k) \oplus (M', c(M'))$
 - Note: we are re-using an IV, but that's ok according to the WEP specification

Summary: WEP is no good

- A tenet of security protocol design: “don’t do it”
- And after all this, I actually recommend running WEP
 - It does create a barrier to the casual hacker
 - It doesn’t add much of a performance hit
 - It does give you legal recourse

Next Time: It gets even worse

- Turns out that using RC4 the way WEP does is bad
 - Ugh
- Next lecture we'll see an attack on WEP based on RC4
 - It's quite technical but very very cool