

# Course 3: Network Security, Section 7

Pascal Meunier, Ph.D., M.Sc., CISSP

May 2004, updated July 30, 2004

Developed thanks to the support of Symantec Corporation,  
NSF SFS Capacity Building Program (Award Number 0113725)  
and the Purdue e-Enterprise Center

Copyright (2004) Purdue Research Foundation. All rights reserved.



## Course 3 Learning Plan

- Architecture
- Physical and link layer
- Network layer
- Transport layer
- Application layer: DNS, RPC, NFS
- Application layer: Routing
- **Wireless networks**
- More secure protocols: DNSSEC, IPSEC, IPv6

## Learning objectives

- Learn about threats faced by wireless networks
- Understand how encrypted wireless networks can be attacked
- Learn from the mistakes in the design of 802.11b

# Wireless Networks

- Wireless Threats
- Antennas
  - Directionality
  - Range
  - Gain
- Design Weaknesses
- Implementation Weaknesses
- Automated WEP crackers and sniffers
- Alternatives to WEP

## Interesting Wireless Uses

- Burlington Northern and Santa Fe Railway Company (BNSF) US railroad uses Wi-Fi to run 'driverless' trains (Smith 2003).
- Home Depot (Luster 2002), BestBuy (Computerworld 2002) and Lowes (Ashenfelter 2003) were famous for being targetted by hackers sitting in the parking lots and eavesdropping on traffic to cash registers, and even accessing their networks through their wireless access points.
- The Navy was reportedly interested in deploying 802.11b technology to control warships (Cox 2003).

# Wireless Threats

- Medium is open to most attackers in the neighborhood of a wireless node
  - Near-impossibility of establishing a clear physical security boundary
    - ❖ Higher gain antennas can be used to overcome distance or a weak signal
- Remote attackers can aim at:
  - The physical layer
  - The link layer
    - ❖ Media Access Control (MAC)
    - ❖ Logical link
  - The network layer

# Threats

- DoS attacks
  - Jamming
  - Fake collisions (Request to send, see slides on CSMA/CA)
  - Amplification
- Integrity attacks
  - Packets captured, modified and reinjected
- Confidentiality attacks
  - Capture passwords, authentication tokens, etc...
- Authentication and Accountability attacks
  - Anonymity for attacker
  - Reassign accountability to network or account owners

## Physical Layer

- CIA
- Coverage vs Risk
- Antenna gain vs transmission power

## Question

- Which property of “CIA” (confidentiality, integrity, availability) can’t you guarantee in any wireless network?
- How about a warship that is steered and controlled through wireless networks. What could happen?

## Answer

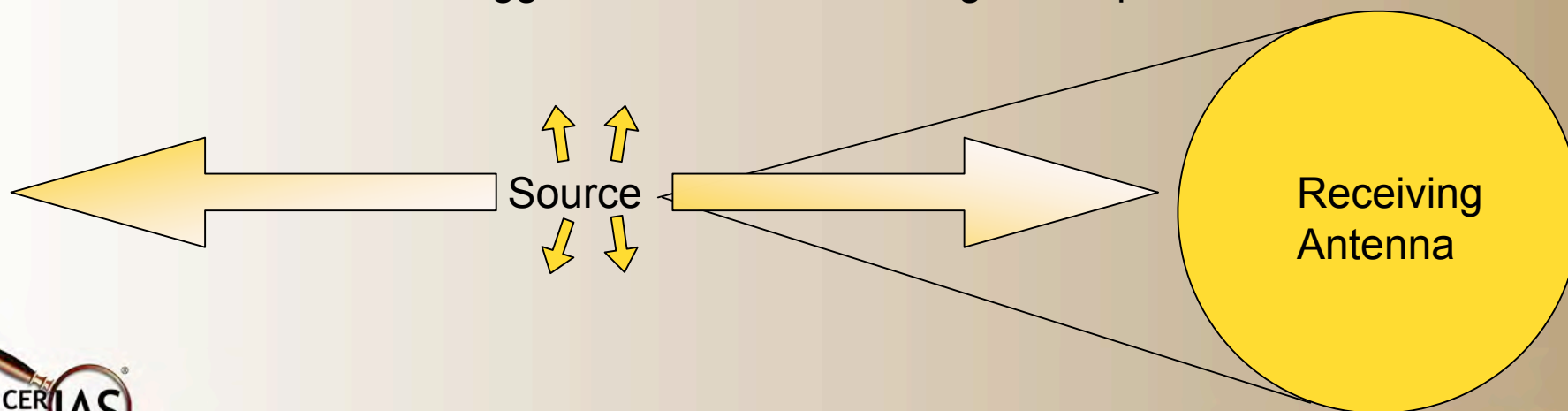
- You can't guarantee availability, because wireless networks can be jammed.
- A warship controlled through a wireless network could stop responding and continue on a bad course (collision or otherwise)

## Wireless Coverage is Risk

- The potential number of locations from which attackers can operate is proportional to the area covered.
- Areas you physically control may not be as risky
- The size of the area is not completely under your control, because attackers can use arbitrarily large antennas.
- However, you can control the amount of power used. How does that affect the risk?

# Wireless Power

- Area of a sphere =  $4\pi r^2$
- Total power is constant
- Power/area decreases  $\approx 1/r^2$
- Big antennas capture more power (more area)
  - Analogy: Lenses
    - ❖ The bigger the lens, the more light is captured



## Wireless Power

- Antenna gain is measured in dB (decibels) as the ratio of power captured compared to a reference antenna.
- Gain usually comes at the cost of increased directionality
  - Power is concentrated in (and captured from) a narrower field

## Antenna Gain (dB)

$$dB = 10 \log_{10} \left( \frac{P_1}{P_2} \right),$$

- Where  $P_2$  is the power captured by the reference antenna
- A gain of 3 dB means captured power is doubled.
- A gain of 10 dB means captured power is increased 10 times.
- A gain of 20 dB means captured power is increased 100 times.

## Variable Power

- Some access points and cards can use varying amounts of power
- Uncommon feature (Cisco, Apple Airport Ex)
- How is the range changed by power?

$$\frac{P_1}{P_2} = \frac{r_1^2}{r_2^2}$$

- How much power do you need to double the range?
  - "r" is the range

# Power Calculations

- Double range needs 4x power
- Equivalent statement:
  - An increase in power of 6 dB doubles the range
- Triple range needs 9x power
- Lower the power to decrease the risk area
- Cisco Aironet Antennas Reference Guide
  - [http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prod/lit/agder\\_rg.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prod/lit/agder_rg.htm)

## Question

- Your wireless network usually has a range of 100 feet. However you are having a (confidential) meeting in a 10' diameter (circular) room but want to use a wireless access point in the room. By how much can you decrease the power to diminish the threats?

## Answer

- A 10'x10' room approximately fits inside a 5' radius sphere.
- $100/5 = 20x$  range reduction
- Power =  $1/(20 \times 20) = 1/400$
- So if the power was 400 mW, 1 mW should now be sufficient.

## Question

- If you want to spy on the meeting mentioned previously, from 100 feet away, what is the gain (in dB) of the antenna you need?

## Answer

$$\begin{aligned}\text{Gain (dB)} &= 10 \log(400) \\ &= 10 \log(4) + 10 \log(100) \\ &= 6 + 20 \\ &= 26 \text{ dB}\end{aligned}$$

# Link Layer

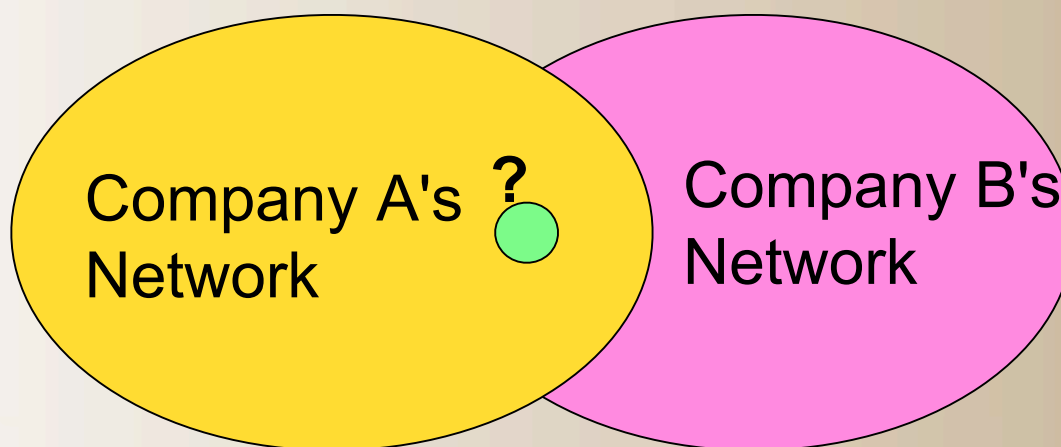
- 802.11b security is focused at the link layer
- Media Access Control
  - MAC address-based access control lists
    - ❖ Refer to the slides on Media Access Control in the link layer
  - CSMA/CA (Collision avoidance)
    - ❖ Refer to the slides on spurious RTS (request to send)
- Logical Link
  - **Logical organization of stations and access points**
  - WEP encryption
  - Network Management frames

## Logical Link

- Wireless networks have two possible architectures
  - Ad-hoc networks
    - ❖ Similar concept: Peer-to-Peer
  - Access-point-based networks (a.k.a. infrastructure mode)
    - ❖ All traffic goes through the access point.
- A station is a member of which network?
  - Association concept

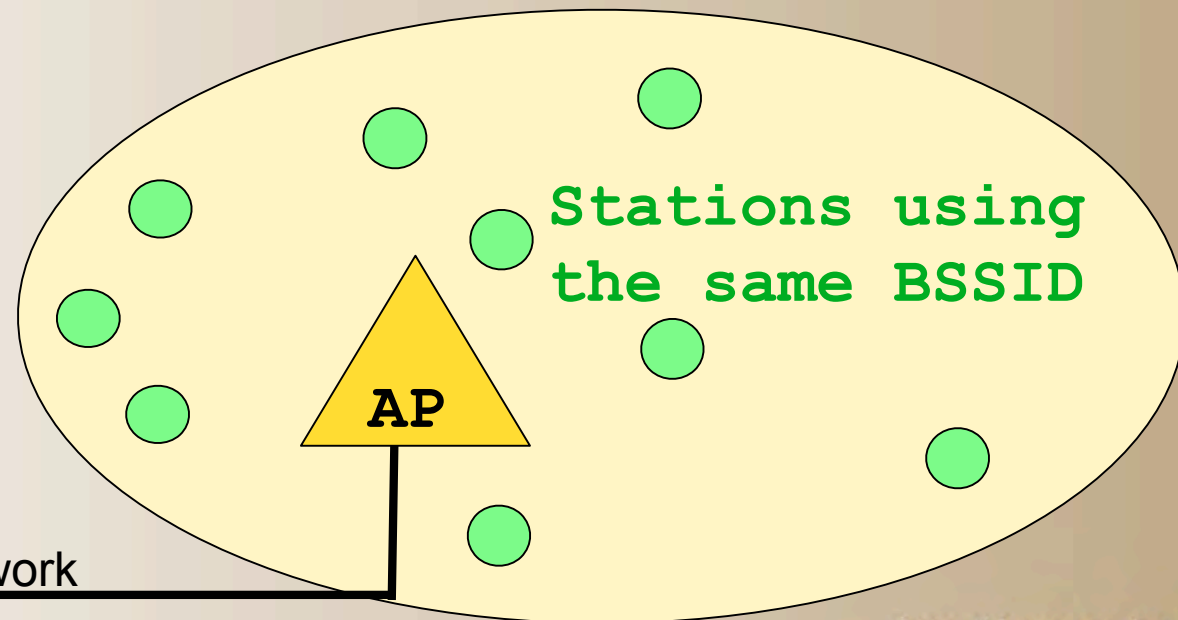
# Definitions

- BSS (Basic Service Set)
  - A collection of stations (a.k.a. nodes) communicating wirelessly together
  - To differentiate between closely BSS and their own, they use a BSSID, which has the format of a MAC address.
    - ❖ All stations in one BSS use the same BSSID to communicate



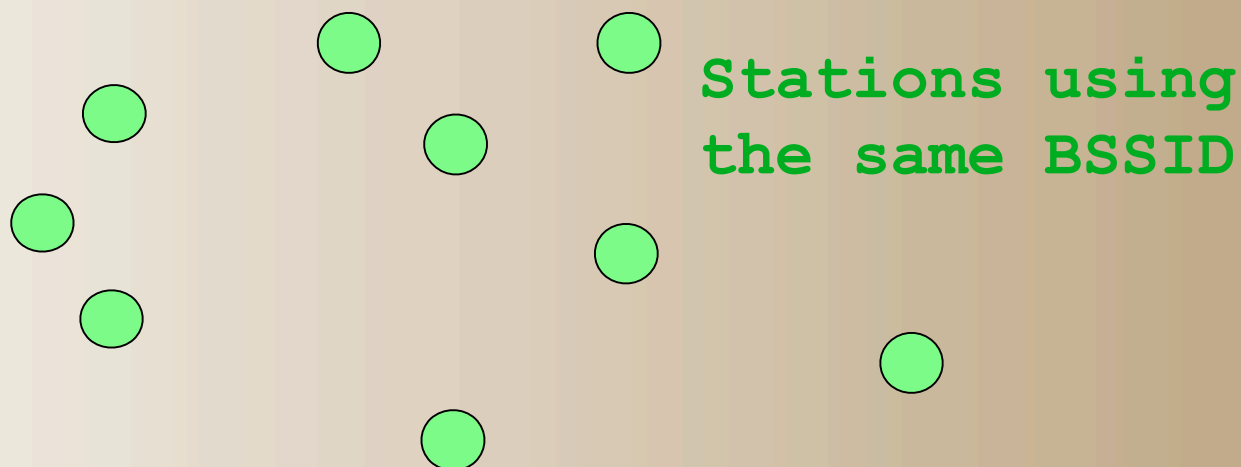
## Infrastructure Mode

- The BSSID is usually the MAC address of the AP (Access Point)
- Sophisticated APs have the capability of handling several BSSes with different BSSIDs, and appear as several virtual APs.



## Ad-hoc Mode

- The stations use a random number as the BSSID
  - The first station selects the BSSID and the others use it



## Definitions (cont.)

- ESS: Extended Service Set
  - Composed of several BSSes joined together.
- SSID: Service Set ID
  - Commonly known as the network name
    - ❖ Human-readable name
  - "ESSID" is sometimes used to refer to the SSID used in the context of an ESS
  - Transparent for the end user
    - ❖ Only aware of the SSID
    - ❖ Traffic in an ESS may be using several different BSSIDs if there are several APs in it.

## Question

- The MAC address of an access point is used for:
  - a) SSID
  - b) ESSID
  - c) BSS
  - d) BSSID

## Question

- The MAC address of an access point is used for:
- a) SSID
- b) ESSID
- c) BSS
- **d) BSSID**

# Beacon Frames

- Beacon Frames broadcast the SSID
  - Help users locate available networks
  - Layer 2 Management frames
  - Networks without BFs are called "closed networks"
    - ❖ Simply means that the SSID is not broadcast anymore
    - ❖ Weak attempt at security through obscurity, to make the presence of the network less obvious
    - ❖ BSSIDs are revealed as soon as a single frame is sent by any member station
    - ❖ Mapping between SSIDs and BSSIDs is revealed by several management frames that are not encrypted

## Is the SSID a Secret?

- Stations looking for an access point send the SSID they are looking for in a "probe request"
- Access points answer with a "probe reply" frame, which contains the SSID and BSSID pair
- Stations wanting to become part of a BSS send an association request frame, which also contains the SSID/BSSID pair in clear text
  - So do re-association requests (see next slides) and their response
- Therefore, the SSID remains secret only on closed networks with no activity
- Conclusion: Closed networks mainly inconvenience legitimate users

# Authentication and Association

- To become part of a BSS, a station must first authenticate itself to the network
  - Then request association to a specific access point
- The access point is in charge of authentication and accepting the association of the station
  - Unless an add-on authentication system (e.g., Radius) is used
- MAC address is trusted as giving the correct identity of the station or access point
  - How can this be abused?

# Abusing MAC Addresses

- A station doesn't know if it is talking to a real access point, or to the same access point every time
  - Access points are not authenticated by stations
    - ❖ Even if they were, the MAC address can be faked
- An access point doesn't know if it is talking to the same station every time

# Authentication and (Dis)Association Attacks

- Any station can impersonate another station or access point and attack or interfere with the authentication and association mechanisms.
  - As these frames are not encrypted, the difficulty is trivial
- Disassociation and deauthentication frames
  - A station receiving one of those frames must redo the authentication and association processes
  - With a single short frame, an attacker can delay the transmission of data and require the station and real access point to redo these processes
    - ❖ takes several frames to perform.

## Disassociation Exploit

- Efficiency was demonstrated by Bellardo (2003)
- Seems to have been used in the "Black Hat" (see below) community prior to that report
  - The tool "KisMAC" implements it
- Availability is affected
  - can be selective against specific users

**Note:** White Hats should do no harm and obey all the rules;  
Black Hats do whatever they want

# Authentication Modes

- Authentication is done by:
  - a station providing the correct SSID
  - or through "shared key authentication"
    - ❖ Access point and all base stations share a secret encryption key
      - Hard to deploy
      - Hard to change
      - Hard to keep secret
      - No accountability
    - ❖ Requires a station to encrypt with **WEP** (see next slides) a challenge text provided by the access point
    - ❖ An eavesdropper gains both the plaintext and the cyphertext
      - Perform a known plaintext attack
      - This authentication helps to crack WEP encryption!

## Nota Bene: 802.11b and WEP

- Remind yourself through this presentation that 802.11b was designed by professional software and hardware engineers and reviewed by many such.
- Be extremely careful and skeptical about “home-brewed” security and encryption solutions.
  - This is an often repeated mistake

## WEP: Wired Equivalent Privacy

- Cryptographic mechanism used to defend against threats
- Developed without
  - Academic or public review
  - Review from cryptologists
- Has significant vulnerabilities and design flaws
- Only about a quarter to a third of wireless access points use WEP
  - Tam et al. 2002
  - Hamilton 2002
  - Pickard and Cracknell 2001, 2003

# WEP

- WEP is a stream cipher
  - Uses RC-4 to produce a stream of bytes that are XORed with the plaintext
  - The input to the stream cipher algorithm is an "initial value" (IV) sent in plaintext, and a secret key
  - IV is 24 bits long
  - Length of the secret is either 40 or 104 bits, for a total length for the IV and secret of 64 or 128 bits
  - Marketing publicized the larger number, implying that the secret was a 64 or 128 bit number, in a classical case of deceptive advertising
    - ❖ How else can you call a protection that is 16.8 million times weaker than advertised?

# XOR Encryption

- $0 \text{ XOR } 0 = 0$   
 $1 \text{ XOR } 0 = 1$   
 $1 \text{ XOR } 1 = 0$   
 $(z \text{ XOR } y) \text{ XOR } z = y$   
 $(z \text{ XOR } y) \text{ XOR } y = z$   
Works independently of which of  $z$  or  $y$  is the  
“plaintext”, “pad” or the “ciphertext”

# Stream Cipher

- Given an IV and secret key, the stream of bytes (pad) produced is always the same
  - Pad XOR plaintext = ciphertext
- If an IV is ever reused, then the pad is the same
- Knowing all the pads is equivalent to knowing the secret
- Application to WEP:
  - The pad is generated from the combination between the IV and the WEP key passed through RC4
  - Knowing all the pads is equivalent to knowing the 40 or 104-bit secret
    - ❖ "Weak" IVs reveal additional information about the secret

## Pad-Collection Attacks

- There is (should be) a different pad for every encrypted packet that is sent between AP and a station
- By mapping pads to IVs, we can build up a table and skip the RC4 step
  - The stream is never longer than 1500 bytes (the maximum Ethernet frame size)
  - The 24 bit-IV provides 16,777,216 ( $256^3$ ) possible streams, so all the pads can fit inside 25,165,824,000 bytes (23.4 GB)
- We never have to have the WEP Key
  - Once we have a complete table, it's as good as having the WEP key.

# Cracking WEP

- Passive attacks
  - The presence of the attacker does not change traffic, until WEP has been cracked
- Active attacks
  - Active attacks increase the risk of being detected, but are more capable.
  - If an active attack is reasonable (i.e., the risk of detection is disregarded), the goal is to stimulate traffic
    - ❖ Collect more pads and uses of weak IVs
    - ❖ Some attacks require only one pad.

## How Authentication Helps Collecting Pads

- Access point sends the plaintext
- Station returns ciphertext
- Mallory computes
  - plaintext XOR ciphertext = pad
  - The IV was in plain text in the packet
  - Mallory now has a pad and matching IV
- Mallory can now authenticate!
  - Access point sends another plaintext challenge
  - Mallory chooses to use the same IV and pad
  - Returns Pad XOR plaintext = ciphertext

## Disassociation Attack to Collect Pads

- Active attack
- Keep forcing stations to re-authenticate and reveal more pads by using different IVs

## Faking Being an Access Point

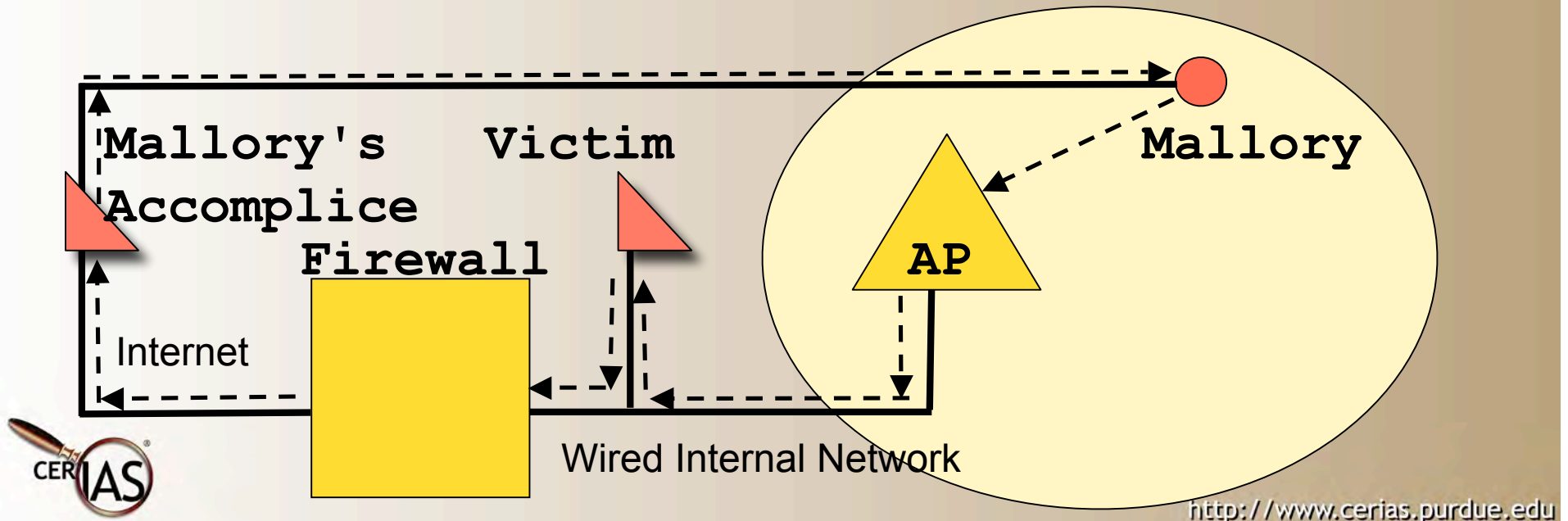
- An attacker can also pretend to be an access point
- Run a cycle of authentication and deauthentication to collect all the pads from other stations
- Works even if the real access points do not require shared key authentication
  - Attacker can require it while faking being an access point

# "Single Pad" Attacks

- Exploits based on knowing a single encryption pad and IV
  - Smurf
  - TCP SYN flood
  - UDP attacks

# Defeating Firewalls with Single Pad Attacks

- Access Point behind a firewall
- Mallory sends packets to Victim, who believes they come from Mallory's accomplice (replies)
- Mallory's accomplice forwards packets to Mallory



## Results

- UDP replies can be obtained unencrypted
- TCP sessions can be established with sensitive services intended to be protected by the firewall
- Intrusion detection systems will most likely ignore responses originating from internal hosts
  - the attacks can proceed undetected at this level
- For all practical purposes, in this configuration WEP has been completely defeated.

## Defenses

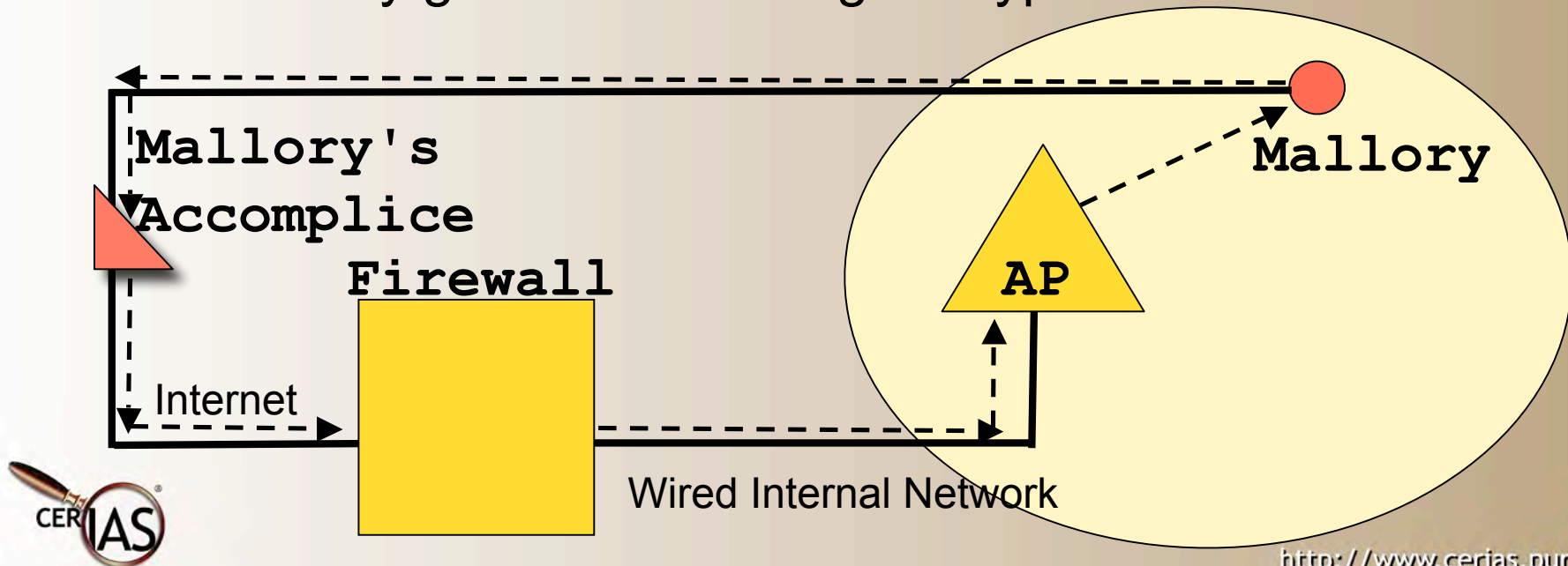
- Provide a firewall for the wireless network with a rule to refuse packets that do not contain source addresses part of the wireless network's range
- Connect access points outside the internet firewall (as if they were part of the internet).
  - Can also negate some advantages of the wireless network for legitimate users

## Administrative Access

- Some access points allow administrative access from the wireless network
- Or offer services on a UDP port (e.g., Apple base stations listen on UDP port 192)
- One-packet attacks directed against these services could exploit vulnerabilities
  - disable the access point or make it difficult to use
- Administrative access to access point should be disabled from the wireless network
  - Not all access points support this feature.

## More Pad Collection Attacks

- Pads collected by disassociation attacks have a limited length
- Mallory sends packets to himself (or to another wireless station) through an internet accomplice
- Mallory gets the matching encrypted version



## Defense

- Requires a stateful firewall
  - will distinguish and block fake responses by keeping track of whether the destination host really made a prior request to the source IP of the packets
- A variation of the attack allows a more sophisticated attacker to launch chosen plaintext attacks against the encryption itself
  - this attack may be useful against encryptions superseding WEP as well

## Weak Keys (a.k.a. Weak IVs)

- Due to how RC4 is used in WEP, some IVs can reveal information about the secret key
  - Mathematical details out of the scope of this material
- Attack
  - FMS (Fluhrer et al. 2001) cryptographic attack on WEP
  - Practicality demonstrated by Stubblefield et al. (2001)
  - Collection of the first encrypted octet of several million packets.
  - Exploits
    - ❖ WEPcrack (Rager 2001)
    - ❖ Airsnort (Bruestle et al. 2001)
  - Key can be recovered in under a second (after collecting the data).

## Defenses

- Some wireless cards no longer generate weak IVs (given a secret, weak IVs can be listed; WEPcrack can do this)
- Some Lucent devices are known to have stopped generating weak IVs (binaervarianz 2003)
- Other vendors should be able to do the same, and make this attack ineffective
  - Which Symantec products use WEP and could stop generating weak IVs?

# Integrity Attacks

- What if Mallory modified a captured packet and resent it on the wireless network?
- IP destination address always in the same location
  - Modify packet so a copy is sent to Mallory's accomplice
    - ❖ Accomplice receives the decrypted packet
- Based on a CRC checksum weakness (Borisov 2001)
  - Given the knowledge of (part of) the plaintext, a WEP-protected message can be changed at will
  - Mallory needs only to guess the relevant IP address
    - ❖ Or part of it, if Mallory's accomplice can sniff traffic on destination network

## Defenses

- Use another encryption layer, such as SSL (https) or ssh

# Implementation Weaknesses

- Restricted IV selection
  - Some access points (old Cisco firmware, notably) produced IVs using only 18 of the 24-bit space
  - Lowered the storage requirement for all pads from 23.4 GB to a mere 366 MB (Meunier et al. 2002)
- Poor randomness for IVs
  - IVs being used more often (reuses of the same pad)
  - Sequential generation allow complete collection faster
- Newsham 21-bit attack

## Implementation Issues

- Newsham 21-bit attack
  - Some manufacturers generate WEP keys from text, in an effort to increase ease-of-use
  - But the algorithm used produces only keys in a 21-bit space instead of 40-bit
    - ❖ Brute force cracking of WEP is  $2^{19}$  (524,288) times faster
    - ❖ Takes less than a minute on commodity hardware (Newsham 2001)
  - Exploits
    - ❖ The tool KisMAC implements this attack
      - According to the tool's documentation, Linksys and D-link products seemed to be vulnerable, but not 3Com and Apple
        - » Are Symantec products vulnerable?

## Automated WEP Crackers and Sniffers

- AiroPeek (Commercial)
  - Easy-to-use, flexible and sophisticated analyzer
- WEPCrack, AirSnort
  - Implementations of the FMA attack
- NetStumbler
  - This is a popular network discovery tool, with GPS support. It does not perform any cracking. A MacOS equivalent is named "iStumbler".
- KisMAC
  - This is a MacOS X tool for network discovery and cracking WEP with several different methods
- Kismet
  - swiss-army knife

# LEAP: The Lightweight Extensible Authentication Protocol

- Proprietary, closed solution
  - was stated (without much details) by Cisco as unaffected by WEP vulnerabilities (Cisco 2002).
- LEAP conducts mutual authentication
  - client is assured that the access point is an authorized one
  - Uses per-session keys that can be renewed regularly
    - ❖ Makes the collection of a pad or weak IVs more difficult
    - ❖ Secret key can be changed before the collection is complete
  - The user is authenticated, instead of the hardware
    - ❖ MAC address access control lists are not needed
  - LEAP requires an authentication server (RADIUS) to support the access points

# LEAP Attacks

- Dictionary attacks
  - Password-based scheme
  - Requires user passwords be guessable (Wright 2003)
- LEAP access points don't use weak IVs
  - Use MS-CHAP v2, show the same weaknesses as MS-CHAP (Wright 2003)
  - There are many variants of the Extensible Authentication Protocol, such as EAP-TLS and PEAP.

# WPA

- Wi-Fi Protected Access
  - stop-gap solution that solves issues related to the WEP encryption itself
    - ❖ IVs are larger (48 bits instead of 24)
    - ❖ Shared key is used more rarely
      - Used to negotiate and communicate "temporal keys"
    - ❖ "Temporal keys" are used to encrypt packets instead
  - Doesn't solve issues with the management frames
  - Collision Avoidance mechanism can still be exploited
  - Can be supported by most of the 802.11b hardware

# Questions or Comments?

---

-

## About These Slides

- You are free to copy, distribute, display, and perform the work; and to make derivative works, under the following conditions.
  - You must give the original author and other contributors credit
  - The work will be used for personal or non-commercial educational uses only, and not for commercial activities and purposes
  - For any reuse or distribution, you must make clear to others the terms of use for this work
  - Derivative works must retain and be subject to the same conditions, and contain a note identifying the new contributor(s) and date of modification
  - For other uses please contact the Purdue Office of Technology Commercialization.
- Developed thanks to the support of Symantec Corporation

# **Pascal Meunier** **pmeunier@purdue.edu**

Contributors:

Jared Robinson, Alan Krassowski, Craig Ozancin, Tim Brown, Wes Higaki, Melissa Dark, Chris Clifton, Gustavo Rodriguez-Rivera

