Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

Wireless Security

Wireless Security

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- What is Wireless Security?
- The usual: confidentiality, integrity, availability?
- Or Butler Lampson's "Gold" (Au) standard: authentication, authorization, audit?
- Both!

Confidentiality

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Obvious danger — it's easy to intercept traffic
- Obvious countermeasure — cryptography
- But it's harder to use here than it looks

Integrity

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- At first glance, integrity seems ok
- This is radio — how can an attacker change messages in mid-packet?
- Solution: the “Evil Twin” (or “Sybil”) attack

Wireless Architecture

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- The obvious architecture is pure peer-to-peer — each machine has a radio, and talks directly to any other machine
- In fact, 802.11 (WiFi) can work that way, but rarely does
- More common scenario: *base stations* (also known as access points)

Access Points

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- An ordinary wireless node *associates* with an access point (AP)
- More precisely, it associates with the AP having a matching network name (if specified) and the strongest signal
- If another AP starts sending a stronger signal (probably because the wireless node has moved), it will reassociate with the new access point
- All transmissions from the laptop go to the access point
- All transmissions to the laptop come from the access point

Which AP?

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Which AP is your laptop associated with?
- Which network (SSID)?
- Many people know neither
- "My ISP is NETGEAR"
- Those who specify anything specify the SSID

The Evil Twin Attack

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Simplest way: carry an access point with you
- Simpler solution: many laptops can emulate access points
- On Linux, use

  ```
  iwconfig eth0 mode Master
  ```

- Force others to associate with your laptop, and send you all their traffic...

Why This Works

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Conventionally, we worry about authenticating the client to the server
- Here, we need to authenticate the server to the client
- The infrastructure wasn't designed for that; more important, users don't expect to check for it (and have no way to do so in any event)

Integrity Attacks

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- We now see how to do integrity attacks
- We don't tinker with the packet in the air, we attract it to our attack node
- You don't go through strong security, you go around it

Availability

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Simple version: black-hole evil twin
- Sophisticated version: battery exhaustion

Black Holes

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Emulate an access point
- Hand out IP addresses
- Do nothing with received packets
- More subtly, drop 10-15% of them — connections will work, but *very* slowly

Battery Exhaustion

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

" Wi-Fi is also a power-hungry technology that can cause phone batteries to die quickly in some cases, within an hour or two of talk time.

When you turn on the Wi-Fi it does bring the battery life down, said Mike Hendrick, director of product development for T-Mobile."

New York Times, 27 November 2006

Battery Exhaustion

Wireless Security
Wireless Security
Confidentiality
Integrity
Wireless Architecture
Access Points
Which AP?
The Evil Twin Attack
Why This Works
Integrity Attacks
Availability
Black Holes
Battery Exhaustion
Battery Exhaustion
WEP
War-Driving
Network Access Control

- Send your enemy large "ping" packets
- The reply packets will be just as big — and transmitting such packets uses a lot of power
- The more you transmit, the more power — often battery power — you use up

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

WEP

WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application

- It was obvious from the start that some crypto was needed
- Choice: WEP — *Wireline Equivalent Privacy* for 802.11 netorks
- Many different mistakes
- Case study in bad crypto design

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

CS @CU

Datagrams and Stream Ciphers

Wireless Security

WEP

WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application

Datagrams and Stream Ciphers

Key Setup

Key Setup for WEP

Cryptanalysis of RC4

IV Replay

Packet Redirection

Checksums

The Biggest Flaw in WEP

What WEP Should Have Been

War-Driving

Network Access Control

- WEP uses RC4 because RC4 is very efficient
- But 802.11 is datagram-oriented; there's no inter-packet byte stream to use

$\Rightarrow$ Must rekey for every packet

- But you can't reuse a stream cipher key on different packets...

Key Setup

Wireless Security

WEP

WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application

Datagrams and Stream Ciphers

Key Setup

Key Setup for WEP

Cryptanalysis of RC4

IV Replay

Packet Redirection

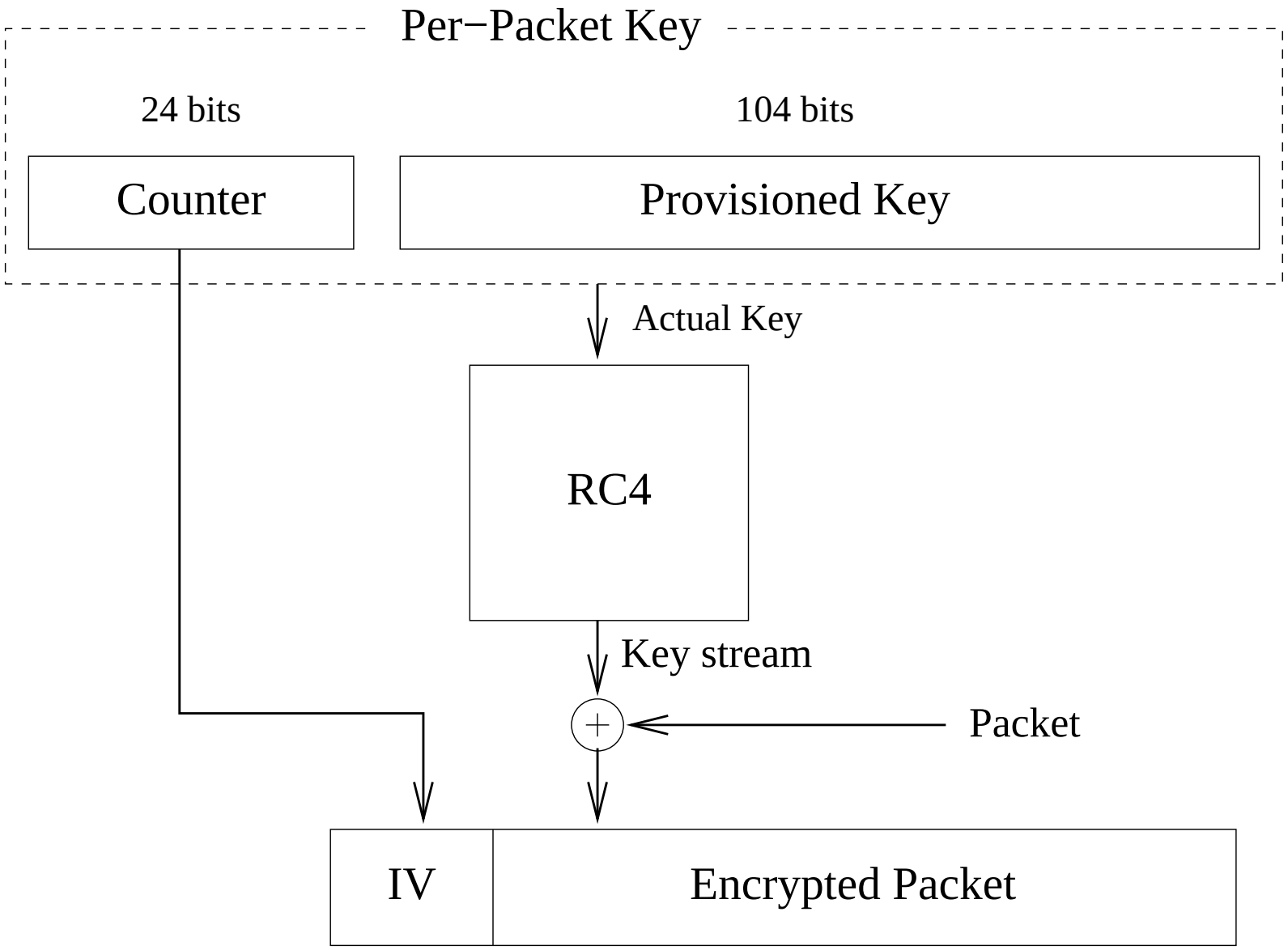
Checksums

The Biggest Flaw in WEP

What WEP Should Have Been

War-Driving

Network Access Control



Key Setup for WEP

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- Each WEP node keeps a 24-bit packet counter (the IV)
- Actual cipher key is configured key concatenated with counter
- Two different flaws...
- 2^{24} packets isn't that many — you still get key reuse when the packet counter overflows
- RC4 has a cryptanalytic flaw
- But it's worse than that

Cryptanalysis of RC4

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- In 2001, Fluhrer, Mantin and Shamir showed that RC4 could be cryptanalyzed if the keys were "close" to each other — a *related key* attack
- Because of the IV algorithm, they are close in WEP
- Key recovery attacks are feasible and have been implemented

IV Replay

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- Suppose you recover the complete plaintext of a single packet
- You can generate new packets that use the same counter
- Receiving nodes don't — and can't — check for rapid counter reuse
- Indefinite forgery!

Packet Redirection

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- Suppose you know (or can guess) the destination IP address of a packet
- Because RC4 is a stream cipher, you can make controlled changes to the plaintext by flipping ciphertext bits
- Flip the proper bits to send the packet to you instead, and reinject it

Checksums

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- WEP does use a checksum
- However, it's a CRC rather than a cryptographic hash
- It's also unkeyed
- Result: it's feasible to compensate for plaintext changes without disturbing the checksum

The Biggest Flaw in WEP

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- There's no key management; all users at a site always share the same WEP key.

$\Rightarrow$ You can't rekey when the counter overflows

$\Rightarrow$ Everyone shares the same key; if it's cryptanalyzed or stolen or betrayed, everyone is at risk

$\Rightarrow$ It's all but impossible to rekey a site of any size, since everyone has to change their keys simultaneously and you don't have a secure way to provide the new keys

What WEP Should Have Been

Wireless Security
WEP
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application
Datagrams and Stream Ciphers
Key Setup
Key Setup for WEP
Cryptanalysis of RC4
IV Replay
Packet Redirection
Checksums
The Biggest Flaw in WEP
What WEP Should Have Been
War-Driving
Network Access Control

- Use a block cipher in CBC mode
- Use a separate key per user, plus a key identifier like the SPI
- Provide dynamic key management
- WPA — WiFi Protected Access — is better than WEP; forthcoming wireless security standards will use AES.

Wireless Security
WEP
War-Driving
War-Driving
Unprotected Networks!
The Consequences
Network Access Control

War-Driving

War-Driving

Wireless Security
WEP
War-Driving
War-Driving
Unprotected Networks!
The Consequences
Network Access Control

- Put a laptop in network (SSID) scanning mode
- Drive around a neighborhood looking for access points
- Perhaps include a GPS receiver to log locations
- Detect presence or absence of WEP
- Name from movie “War Games”

Unprotected Networks!

Wireless Security
WEP
War-Driving
War-Driving
Unprotected Networks!
The Consequences
Network Access Control

- Statistics show that only O(1/3) use even WEP
- The rest tend to be wide open
- Many people don't change or hide the SSID

The Consequences

Wireless Security
WEP
War-Driving
War-Driving
Unprotected Networks!
The Consequences
Network Access Control

- Some incidence of theft of service
- (Is it war-driving a crime? Unclear under US law)
- Sometimes done to hide criminal activity

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

Network Access Control

CS @CU

No Perimeter

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- The fundamental difference: there's no physical boundary
- On a wired net, physical access control can compensate for lack of technical security
- Most of the attacks are the same, for wired or wireless nets
- But physical perimeters let us take shortcuts

Associations

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- Wired nets don't have a base station that nodes associate with at layer 2
- However, ARP attacks can compensate
- ARP attacks are even harder to detect — there's no pop-up informing you about local Ethernet addresses

Tracing Attacks

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- With wired networks, you can trace an attack to a given switch port
- With wirless networks, you can trace an attack to a given AP, but the AP might serve hundreds or thousands of square meters
- No good way to trace — all you can do is log and block MAC addresses

MAC Address Filtering

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- Can allow or block endpoints based on MAC address
- However – MAC address spoofing is pretty easy
- Evade blocks and/or impersonate accepted hosts
- What's accepted? Look for machines that receive non-SYN TCP packets

Clayton's Spoofing Attack

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- Impersonate a known-good IP and MAC address
- TCP replies will go to the real owner and the fake one
- The real one will send out a TCP RST packet
- Build a circuit that listens for the bit pattern of the RST and sends a jam signal instead

Windows XP SP2 and Spoofing

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- With SP2, the built-in firewall blocks most inbound packets
- In particular, it only allows in replies to outbound packets
- The TCP reply packets don't match any outbound connections
- TCP never sees the reply, and hence doesn't generate RST
- No need for Clayton's attack

Network Access Control

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- Fundamentally, the problem is network access control
- We have none with wireless
- Usual solution: let people onto your network, but require some sort of Web-based login

Evil Twin Redux

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- Set up your evil twin in a hotspot
- Intercept the login session and/or the registration
- Registration often involves a credit card...

The Gold Standard

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- No authentication at the WEP layer; higher-layer authentcation susceptible to evil twin attack
- Authorization based on MAC address and WEP key; both are vulnerable
- Rarely any logging for audit
- Oops...

Living with Wireless

Wireless Security
WEP
War-Driving
Network Access Control
No Perimeter
Associations
Tracing Attacks
MAC Address Filtering
Clayton's Spoofing Attack
Windows XP SP2 and Spoofing
Network Access Control
Evil Twin Redux
The Gold Standard
Living with Wireless

- For residential use, turn off SSID broadcast
- (Hard to do in an enterprise)
- Put your wireless net outside the firewall
- Use WEP — it's still (marginally) better than nothing
- Better yet, use WPA
- Use end-to-end crypto
- Check the certificate on registration or login pages