

# Wireless Security

# Confidentiality

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

# Wireless Security

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

# Integrity

- At first glance, integrity seems to be sufficient
- 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 (Wi-Fi) can work that way, but rarely does
- More common scenario: *base stations* (also known as access points)

5 / 40

## 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

7 / 40

## 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 re-associate 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

6 / 40

## 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. . .

8 / 40

## 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)

## 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

## 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

## 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

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

13 / 40

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

War-Driving

Network Access

Control

## WEP

15 / 40

## 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

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

14 / 40

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

War-Driving

Network Access

Control

## 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 networks
- Many different mistakes
- Case study in bad crypto design

16 / 40

## 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

Control

- WEP uses RC4 because RC4 is very efficient
  - But 802.11 is datagram-oriented; there's no inter-packet byte stream to use
- ⇒ Must re-key for every packet
- But you can't reuse a stream cipher key on different packets...

17 / 40

## 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

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 flaw that allows effective cryptanalysis to be applied
- But it's worse than that

19 / 40

## 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

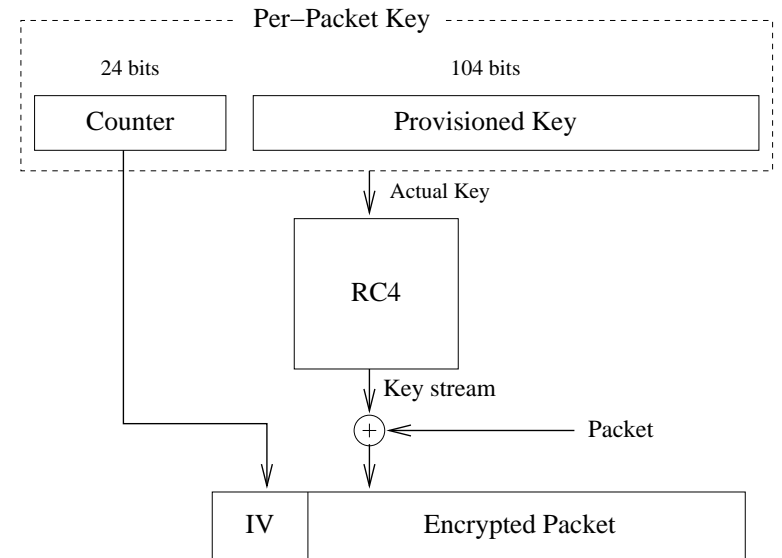
The Biggest Flaw in WEP

What WEP Should Have Been

War-Driving

Network Access Control

Control



18 / 40

## 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

Control

- In 2001, Fluhrer, Mantin and Shamir showed that RC4 could be 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

20 / 40

## IV Replay

- Suppose you recover the complete plain-text 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!

21 / 40

## Checksums

- WEP does use a check-sum
- However, it's a CRC rather than a cryptographic hash
- It's also un-keyed
- Result: it's feasible to compensate for plain-text changes without disturbing the checksum

23 / 40

## Packet Redirection

- 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 plain-text by flipping cipher-text bits
- Flip the proper bits to send the packet to you instead, and re-inject it

22 / 40

## The Biggest Flaw in WEP

- There's no key management; all users at a site always share the same WEP key.
  - ⇒ You can't re-key when the counter overflows
  - ⇒ Everyone shares the same key; if cryptanalysis techniques are applied, the key is stolen or betrayed, everyone is at risk
  - ⇒ It's all but impossible to re-key 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

24 / 40

## 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 — Wi-Fi Protected Access — is better than WEP; forthcoming wireless security standards will use AES.

25 / 40

## 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”

27 / 40

Wireless Security

WEP

War-Driving

War-Driving

Unprotected

Networks!

The Consequences

Network Access

Control

## War-Driving

26 / 40

## 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

28 / 40

# 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

# 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 perimeter let us take shortcuts

- [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

# 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

- With wired networks, you can trace an attack to a given switch port
- With wireless 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

## Clayton's Spoofing Attack

- 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

## MAC Address Filtering

- 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

## Windows XP SP2 and Spoofing

- With SP2, the built-in firewall blocks most in-bound 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

- 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

## The Gold Standard

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

## Evil Twin Redux

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

## 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