CE 817 - Advanced Network Security
Wireless Security

Lecture 23

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

Wireless Security

- What is Wireless Security?
- The usual: confidentiality, integrity, availability?

Confidentiality

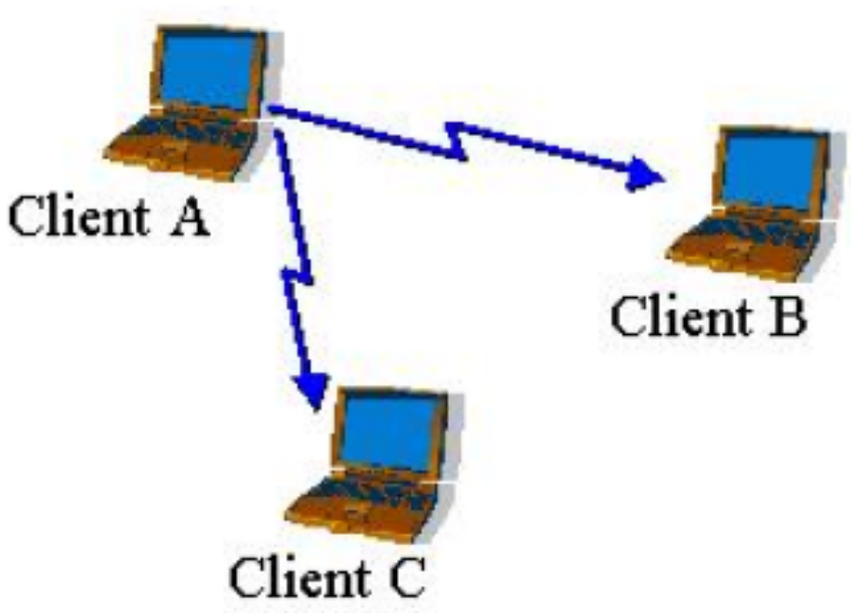
- Obvious danger — it’s easy to intercept traffic
- Obvious countermeasure — cryptography

Integrity

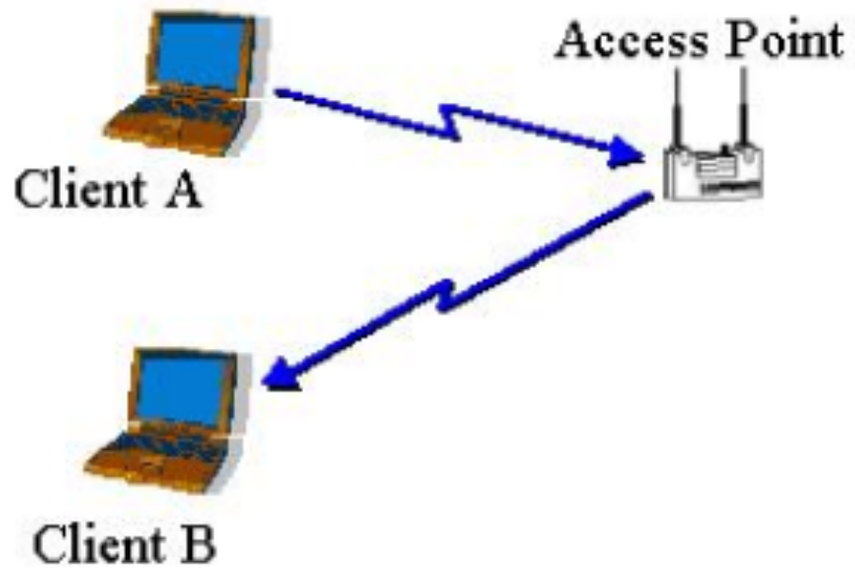
- At first glance, integrity seems ok
- This is radio — how can an attacker change messages in mid-packet?
- Solution: the “Evil Twin” (or “Sybil”) attack

Wireless Architecture

- 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)



IBSS (ad hoc) mode



BSS (infrastructure) mode

Access Points

- 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

Access Point SSID

- Service Set Identifier (SSID) is the “name” of the access point
  - By default, access point broadcasts its SSID in plaintext “beacon frames” every few seconds
- Default SSIDs are easily guessable
  - Linksys defaults to “linksys”, Cisco to “tsunami”, etc.
    - This gives away the fact that access point is active
- Access point settings can be changed to prevent it from announcing its presence in beacon frames and from using an easily guessable SSID
  - But then every user must know SSID in advance

Example

- You could find defaults easily:

  Netgear 802.11 DS products, ME102 and MA401

  Default SSID: Wireless

  Default Channel: 6

  Default IP address: 192.168.0.5

  Default WEP: Disabled

  Default WEP KEY1: 11 11 11 11 11

  Default WEP KEY2: 20 21 22 23 24

  Default WEP KEY3: 30 31 32 33 34

  Default WEP KEY4: 40 41 42 43 44

  Default MAC: 00:30:ab:xx:xx:xx

Which AP?

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

The Evil Twin Attack

- 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

- 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

- 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

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

Black Holes

- 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

- “ 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

- 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

WEP

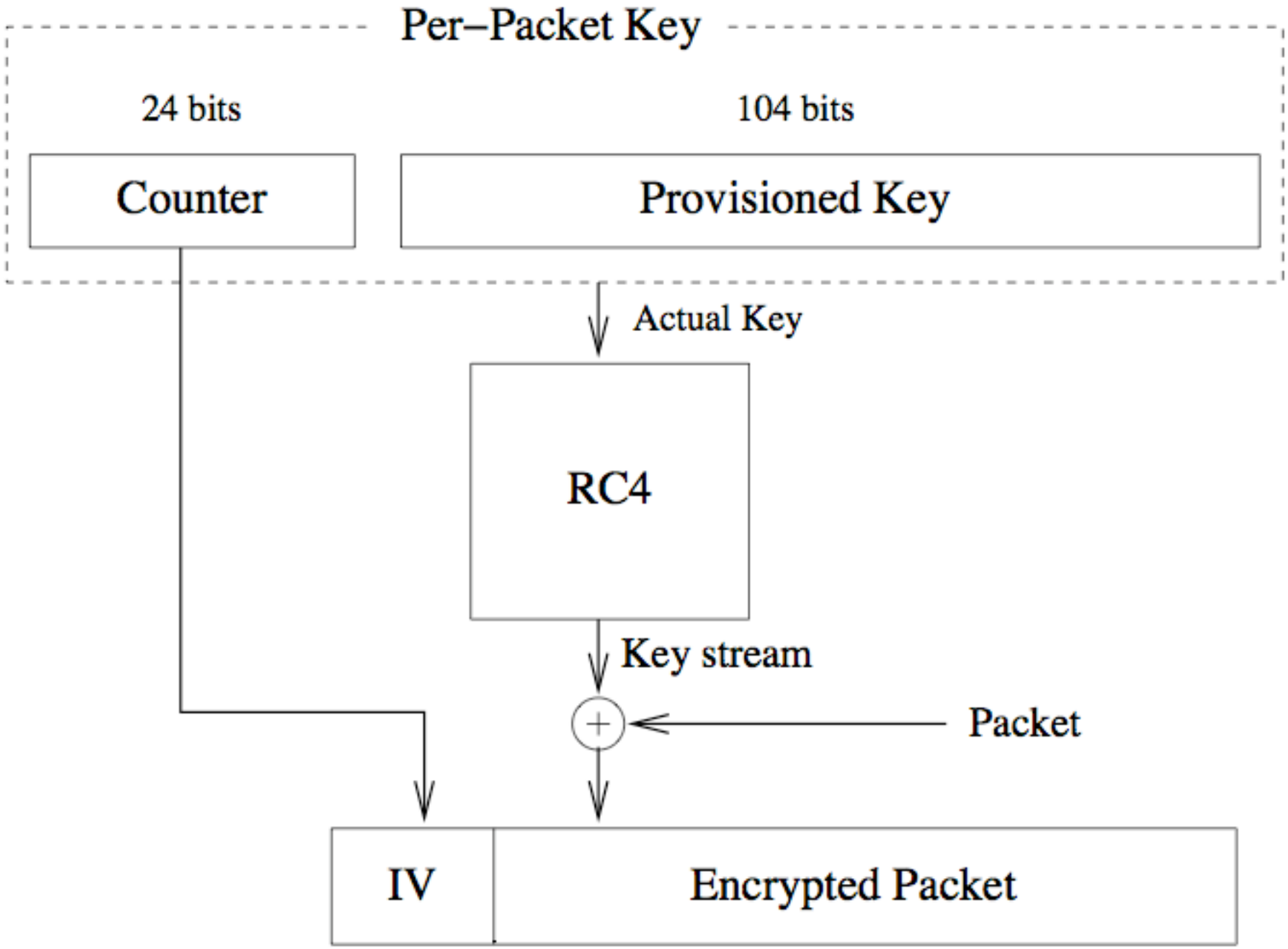
WEP — Using a Flawed Cipher in a Bad Way for the Wrong Application

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

Datagrams and Stream Ciphers

- WEP uses RC4 because RC4 is very efficient
- But 802.11 is datagram-oriented
- --> Must rekey for every packet
- But you can’t reuse a stream cipher key on different packets. . .

Key Setup


Per–Packet Key
24 bits
104 bits
Counter
Provisioned Key
Actual Key
RC4
Key stream
Packet
IV
Encrypted Packet

Key Setup for WEP

- 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

- 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

- 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

- 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

- 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

- There’s no key management; all users at a site always share the same WEP key.
- --> You can’t rekey when the counter overflows
- --> Everyone shares the same key; if it’s cryptanalyzed or stolen or betrayed, everyone is at risk
- --> 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

- 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.

War-Driving

War-Driving

- 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

Unprotected Networks!

- 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

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

Network Access Control

No Perimeter

- 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

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

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

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

Windows XP SP2 and Spoofing

- 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

- 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

- Set up your evil twin in a hotspot
- 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

Acknowledgments/References

- [Bellovin06] COMS W4180 — Network Security Class Columbia University, Steven Bellovin, 2006.
- [Shmatikov] CS 378 - Network Security and Privacy, Vitaly Shmatikov, University of Texas at Austin, Fall 2007.