Wireless Network Security

- Wireless networks are “just like” other networks
- Except . . .
  - Almost always broadcast
  - Generally short range
  - Usually supporting mobility
  - Often very open

Types of Wireless Networks

- 802.11 networks
  - Variants on local area network technologies
- Bluetooth networks
  - Very short range
- Cellular telephone networks
- Line-of-sight networks
  - Dedicated, for relatively long hauls
- Satellite networks

The General Solution For Wireless Security

- Wireless networks inherently less secure than wired ones
- So we need to add extra security
- How to do it?
- Link encryption
  - Encrypt traffic just as it crosses the wireless network
    Decrypt it before sending it along

Why Not End-to-End Encryption?

- Some non-wireless destinations might not be prepared to perform crypto
  - What if wireless user wants protection anyway?
- Doesn’t help wireless access point provide exclusive access
  - Any eavesdropper can use network

802.11 Security

- Originally, 802.11 protocols didn't include security
- Once the need became clear, it was sort of too late
  - Huge number of units in the field
  - Couldn't change the protocols
- So, what to do?

WEP

- First solution to the 802.11 security problem
- Wired Equivalency Protocol
- Intended to provide encryption in 802.11 networks
  - Without changing the protocol
  - So all existing hardware just worked
- The backward compatibility worked
- The security didn’t

What Did WEP Do?

- Used stream cipher (RC4) for confidentiality
  - With 104 bit keys
  - Usually stored on the computer using the wireless network
  - 24 bit IV also used
- Used checksum for integrity

What Was the Problem With WEP?

- Access point generates session key from its own permanent key plus IV
  - Making replays and key deduction attacks a problem
- IV was intended to prevent that
- But it was too short and used improperly
- In 2001, WEP cracking method shown
  - Took less than 1 minute to get key

WPA and WPA2

- Generates new key for each session
- Can use either TKIP or AES mode
- Various vulnerabilities in TKIP mode
- AES mode hasn’t been cracked yet
  - May be available for some WPA
  - Definitely in WPA2

Honeypots and Honeynets

- A *honeypot* is a machine set up to attract attackers
- Classic use is to learn more about attackers
- Ongoing research on using honeypots as part of a system’s defenses

Setting Up A Honeypot

- Usually a machine dedicated to this purpose
- Probably easier to find and compromise than your real machines
- But has lots of software watching what’s happening on it
- Providing early warning of attacks

What Have Honeypots Been Used For?

- To study attackers' common practices
- There are lengthy traces of what attackers do when they compromise a honeypot machine
- Not clear these traces actually provided much we didn't already know

Honeynets

- A collection of honeypots on a single network
  - Maybe on a single machine with multiple addresses
  - More often using virtualization
- Typically, no other machines are on the network
- Since whole network is phony, all incoming traffic is probably attack traffic

What Can You Do With Honeynets?

- Similar things to honeypots
  - But at the network level
- Also good for tracking the spread of worms
  - Worm code typically visits them repeatedly
- Main tool for detecting and analyzing botnets
- Gives evidence of DDoS attacks
  - Through *backscatter*
  - Based on attacker using IP spoofing

Honeynets and Botnets

- Honeynets widely used by security researchers to “capture” bots
- Honeynet is reachable from Internet
- Intentionally weakly defended
- Bots tend to compromise them
- Researcher gets a copy of the bot

Issues With Honeynet Research

- Don’t want captured bot infecting other non-honeynet sites
  - Or performing other attack activities
- So you need to prevent it from attacking out
- But you also need to see its control traffic

What To Do With a Bot?

- When the bot is captured, what do you do with it?
- Typically, analyze it
  - Especially for new types of bots
  - To find weaknesses
  - And to track rest of botnet
- Analysis helpful for tracing “ancestry”

Do You Need A Honeypot?

- Not in the same way you need a firewall
- Only useful if your security administrator spending a lot of time watching things
  - E.g., very large enterprises
- Or if your job is observing hacker activity
- Something that someone needs to be doing
  - Particularly, security experts watching the overall state of the network world
  - But not necessarily you