Hacking WiFi and Bluetooth

Chapter 15

SYBEX

802.11

- **IEEE group responsible for defining interface between wireless clients and their network access points in wireless LANs**
- **First wireless standard was defined in 1997**
- **Standard was responsible for defining three types of transmission at the Physical layer**
  - Diffused infrared : infrared transmission-based
  - Direct sequence spread spectrum (DSSS): radio-based
  - Frequency hopping spread spectrum (FHSS): radio-based

SYBEX

802.11

- Specified WEP as an optional security protocol
- Specified use of 2.4 GHz industrial, scientific, and medical (ISM) radio band
- Mandated 1 Mbps data transfer rate and optional 2 Mbps data transfer rate
- Most prominent working groups: 802.11b, 802.11a, 802.11i, and 802.11g

SYBEX

A Look at 802.11a

- Sets specifications for wireless data transmission of up to 54 Mbps in the 5 GHz band
- Uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS
- Approved in 1999
- Typically restricted to corporate deployments

SYBEX

A Look at 802.11b

- Establishes specifications for data transmission that provides 11 Mbps transmission at 2.4 GHz band
- Sometimes referred to as "WiFi" when associated with WECA-certified devices
- Uses only DSSS
- Approved in 1999
- First widely adopted wireless standard
- Deployed in home, small businesses, and corporations
- Being supplanted slowly by 802.11g and 802.11n

SYBEX

A Look at 802.11g

- Responsible for providing raw data throughput over wireless networks at a throughput rate of 22 Mbps or more
- Draft created in January 2002; final approval in 2003
- Replaced 802.11b in many wireless deployments

SYBEX

A Look at 802.11i

- Responsible for fixing security flaws in WEP and 802.1x
- Hopes to eliminate WEP altogether and replace it with Temporal Key Integrity Protocol (TKIP)
- Ongoing; not yet approved

SYBEX

Wired Equivalent Privacy (WEP)

- Optional security protocol for wireless local area networks defined in the 802.11b standard
- Designed to provide same level of security as a wired LAN
- Not considered adequate security without also implementing a separate authentication process and providing for external key management

SYBEX

Wireless LAN (WLAN)

- **Connects clients to network resources using radio signals to pass data through the ether**
- **Employs wireless access points (APs)**
  - Connected to the wired LAN
  - Acts as radio broadcast stations that transmit data to clients equipped with wireless network interface cards (NICs)

SYBEX

How WEP Functions

- Employs a symmetric key to authenticate wireless devices and to guarantee integrity of data by encrypting transmissions
- Each of the APs and clients must share the same key
- Client sends a request to the AP asking for permission to access the wired network

SYBEX

How WEP Works

- If WEP has not been enabled (default), the AP allows the request to pass.
- If WEP has been enabled, the client begins a challenge-and-response authentication process.

Vulnerabilities of WEP

- **Problems related to the initialization vector (IV) that it uses to encrypt data and ensure its integrity**
  - Can be picked up by hackers
  - Is reused on a regular basis
- **Problems with how it handles keys**
- **Advanced techniques employed by hackers can breech WEP in less than 30 seconds**

SYBEX

Other WLAN Security Loopholes

- **"War" techniques:**
  - War driving
  - War flying
  - War walking
  - War ballooning
- **Unauthorized users can attach themselves to WLANs and use their resources, set up their own access points, and jam the network.**
- **WEP authenticates clients, not users.**
- **Wireless network administrators and users must be educated about inherent insecurity of wireless systems and the need for care.**

SYBEX

Conducting a Wireless Site Survey

1. Conduct a needs assessment of network users.
2. Obtain a copy of the site's blueprint.
3. Do a walk-through of the site.
4. Identify possible access point locations.
5. Verify access point locations.
6. Document findings.

SYBEX

Summary

- The Many Faces of 802.11
- The Role of Wireless Application Protocol (WAP)
- Wired Equivalent Privacy (WEP)

SYBEX