Wireless Systems Security

Last Class – Wrap-up and Closing Thoughts
The Intersection of Wireless and Security

Top-Down Systems Focus

Wireless Communications

Security

Confidentiality
Fraud Prevention
Availability
Integrity
Traffic Flows
Privacy
Access
Identity
Authenticity
“Spoofing”
Jamming

Confidentiality
Fraud Prevention
Availability
Integrity
Traffic Flows
Privacy
Access
Identity
Authenticity
“Spoofing”
Jamming

Aircraft ILS
WLAN
Satellite
Cordless
Public Safety
Military Tactical
Cellular
Paging
Raw news feeds
Broadcast
Short-wave
Military strategic

The intersection of Wireless and Security focuses on systems that are designed to ensure confidentiality, fraud prevention, availability, integrity, traffic flows, privacy, access, identity, authenticity, and avoid "spoofing" and jamming. This includes various wireless technologies such as aircraft ILS, WLAN, satellite, cordless, public safety, military tactical, cellular, paging, raw news feeds, broadcast, short-wave, and military strategic.
RF Spectrum

Typical ranges

- **Ionospheric**
- **Ground wave**
- **Tropospheric ducting**

Propagation modes

- **VLF**
- **LF**
- **MF**
- **HF**
- **VHF**
- **UHF**
- **SHF**

Or [http://www.jsc.mil/images/speccht.jpg](http://www.jsc.mil/images/speccht.jpg) for the military view
CDMA Spreading and Despreading

Spreading factor $\sim \frac{\text{(RF Bandwidth)}}{\text{(Baseband bandwidth)}}$
How Much Security Is Enough?

A security assessment model

Perpetrators

What

Who

How

Where

Assets at Risk

Existing safeguards

Threats

Additional controls

Potential vulnerabilities

Who

What

When?

Why?
One Structured Way of Viewing Security

- Confidentiality
- Integrity
- Availability
- Access Control
- Authentication
- Identification

Security Services
- Security Services
- Security Mechanisms
- Security Infrastructure
One-bit-pad Key Reuse

Knowing he has no other possible attack, interloper hopes $KS_1$ has been reused and tries combining ciphers

$$\text{(KS}_1\text{xor)M}_1 \text{ (xor) (KS}_1\text{xor) M}_2 = \text{(KS}_1\text{xor)KS}_1 \text{ (xor) (M}_1\text{ (xor) M}_2 = M}_1 \text{ (xor) M}_2$$

This is the polyalphabetic encryption of $M_1$ using $M_2$ as a key stream!!
DES as an Example of Encryption Algorithm

plaintext → DES → ciphertext

key variable

64

Initial permutation

Round 1

Round 2

Round 16

IP⁻¹

Key variable

64

56

Key schedule

L  R

L  R

L  R

IP⁻¹

ciphertext

32 32

32 32

32 32

64

ciphertext

56

48

48

48

K1

K2

K16

E

P

S

48

32

32

48

32

48

32

L

R

L

R
Case 1
Terrestrial Microwave RF Telephone Relay System

4 GHz
Analog SSB FDMA
Multichannel Voice traffic
CCS signaling
Washington, DC area
Case 2 – Public Safety Wireless Networks

30-50, 150, 450 MHz (mostly) analog FM
Local municipality control
Separate services (police, fire, EMS)
with little central coordination
Some point-to-point; heavy use of RF repeaters
Case 3 – Military Tactical Radio Systems

30-88 MHz VHF-FM/FSK link
25 kHz channels, 16 kb/s voice/data
Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz transponders. Scrambled video, encrypted audio

Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

Broadcast TV, Long distance communications
Case 5 – Wide Area Wireless Data Services
CDPD, 3G, EDGE, etc.

MacroCell spacing ~5-10 miles at 850 MHz, 3-5 miles at 1900 MHz

850:
Data over AMPS: ~2.4 – 4.8 kb/s
CDPD up to 19.2 kb/s
IS-136: ~8 kb/s

1900:
EDGE/3G: up to 384 kb/s
4G: 5-10 Mb/s?
Case 6 – Wireless LANs
802.11a, b, g

- RC4 stream cipher
- CRC-32 message integrity check
- 24 bit IV
- IV updating optional
- WLAN-wide key variable

Diagram:
- Internet
- Firewall
- Intranet
Case 7 – Wireless Metropolitan Area Networks (W-MANs) 802.16

802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates
The Intersection of Wireless and Security

Top-Down Systems Focus

Wireless Communications

- Aircraft ILS
- WMAN
- Satellite
- Cordless
- Cellular
- Paging
- Raw news feeds
- Broadcast
- Short-wave
- Military strategic
- Terrestrial microwave
- 3G, EDGE, 4G

Security

- Confidentiality
- Availability
- Integrity
- Traffic Flows
- Privacy
- Access
- Identity
- Authenticity
- “Spoofing”
- Jamming

Wireless Communications

- Cellular
- Paging
- Raw news feeds
- Broadcast
- Short-wave
- Military strategic
- Terrestrial microwave
- 3G, EDGE, 4G
Key Points

- **Security:**
  - is best designed in, rather than added on
  - issues must be examined in the broadest context
  - cannot be taken for granted

- The interaction between complex systems is a fertile growth medium for security issues
  - Where does mold tend to grow in homes?

- Wireless systems are generally:
  - New designs (not much field experience)
  - Complex (interactions between varied technologies)
  - Designed with short development cycles
  - Closed systems at introduction

- Broadcast nature of most wireless systems creates issues that wired systems don’t share:
  - Ease of monitoring
  - Potential for jamming
  - Attack from anywhere – difficulty in controlling access to airwaves
A Few Operative Definitions

• Quality is meeting or exceeding customers’ expectations
• Security is meeting or exceeding customers’ expectations *in the presence of the* actions of an adversary
A Few Operative Definitions

- Quality is meeting or exceeding customers’ expectations
- Security is meeting or exceeding customers’ expectations in the presence of the actions of an adversary

- An fool is someone who does not learn from their mistakes
- A genius is someone who learns from other’s mistakes
A Few Operative Definitions

- Quality is meeting or exceeding customers’ expectations.
- Security is meeting or exceeding customers’ expectations in the presence of the actions of an adversary.
- An fool is someone who does not learn from their mistakes.
- A genius is someone who learns from other’s mistakes.
- Effective quality processes do not expect perfection.
- They do expect continuous process improvement.