Wireless Systems Security

EE/NiS/TM-584-A/WS

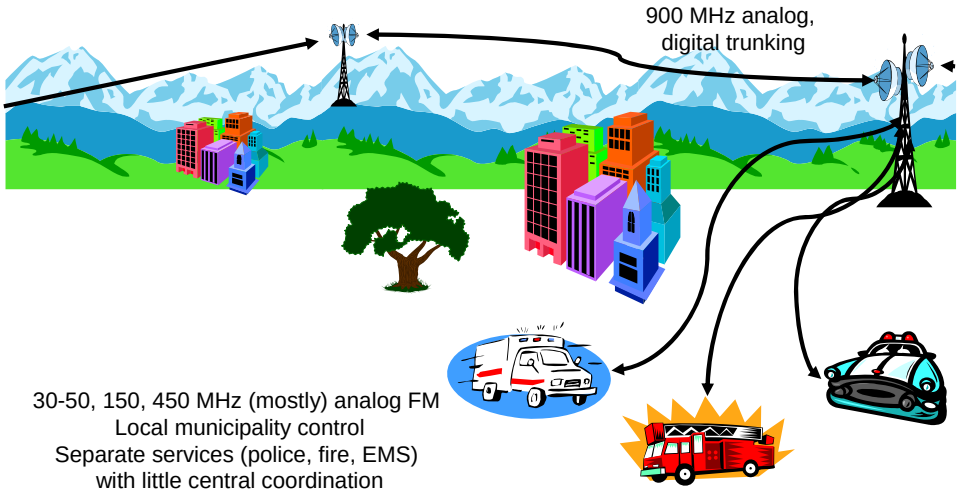
Bruce McNair
bmcnair@stevens.edu

Week 6 - Wrapup

Case Study 2
Summary and observations

At this point, you have completed the discussions for the second case study. I wanted to make some observations about the system we have assessed and summarize the assessment. For the later, I am using assessment results from previous groups who have taken this class. I will add your assessment results to future versions of this class.

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

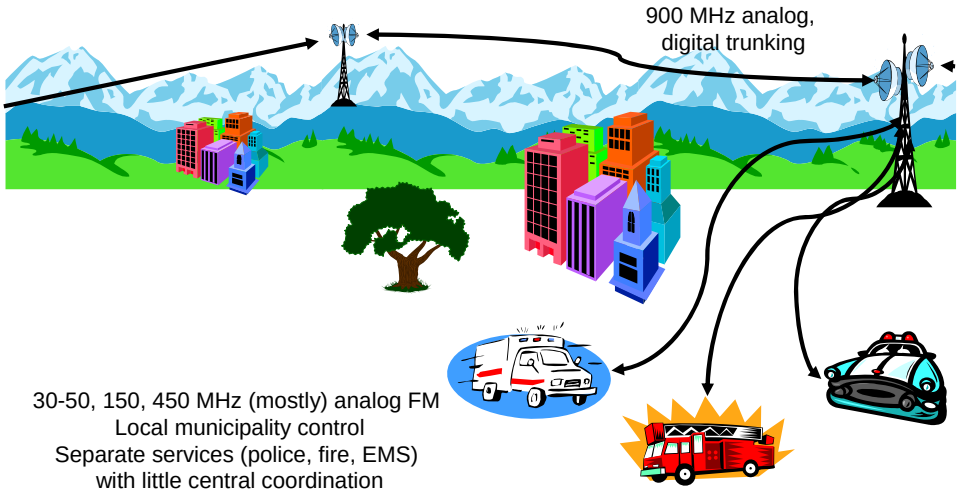
One of the biggest issues with this system is the lack of confidentiality of transmissions. Consider these situations:

(1) Drivers license numbers are personally identification information that, if compromised, would allow one to steal a victim's identity. During traffic stops, these numbers have been routinely read over insecure connections

(2) Fire dispatch transmissions to specific addresses are made in the clear. What better house to target for looting than one that has been damaged, with residents who are more concerned with their safety than security of their possessions?

(3) Although patient names are not associated with medical discussions of patients en route to a hospital, a great deal about a patient's condition is freely broadcast. As the fire dispatch, the ambulance dispatch to a particular address is made in the clear. Monitoring of ambulance transmissions has the potential to compromise sensitive medical information about individuals.

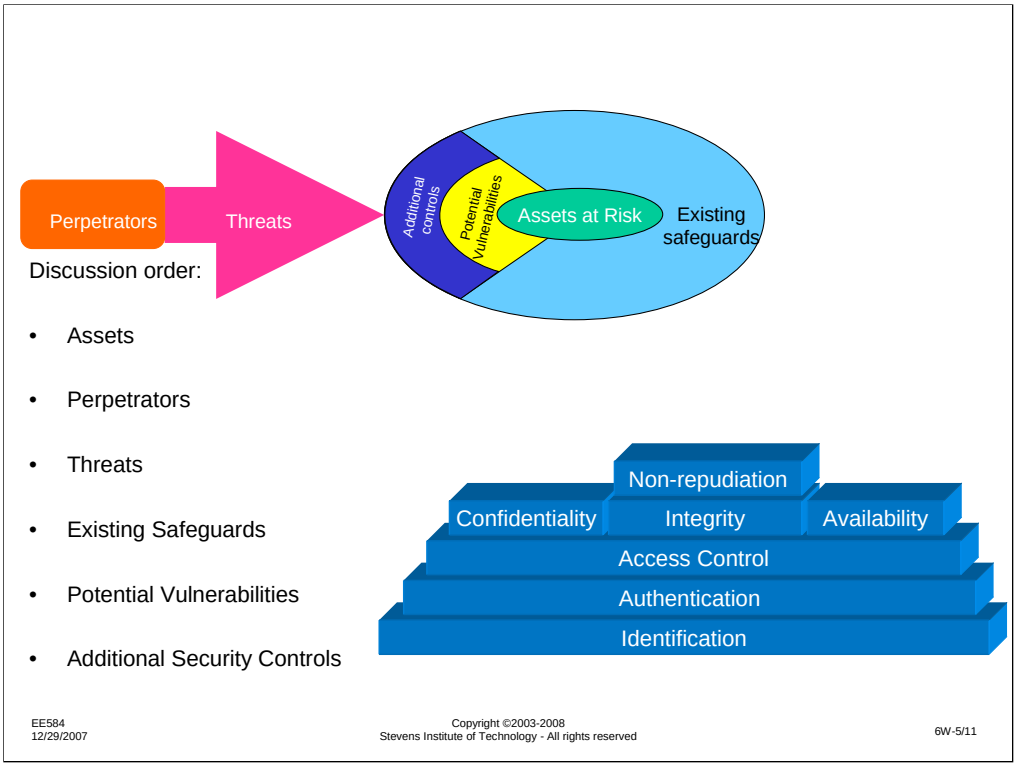
Case 2 – Public Safety Wireless Networks



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

The general lack of interoperability of police, fire and EMS systems across different jurisdictions might not, on the surface, appear to be a security issue, but if the utility of the systems are degraded for important communications, this could be considered to be an availability issue.

As previously noted, this issue was made very clear with the intense activities of public safety services on 9/11/01, but the problem continues today. If the systems cannot be relied on when they are needed most, they fail to meet their requirements.



You have probably observed that the discussion of attacks on a system is easier to engage in than the discussion of protection of the system. This is the point of having formed Red and Blue teams. Without an attack scenario to defend against, it is easy to get overwhelmed with the problem of securing a system. This often leads to complacency about whether the attacks will actually occur.

On the other hand, by going through the thought process of “How might I attack this system?” one begins to appreciate the possibilities. Having thought about methods of successfully attacking a system, one is in a much better position to assess whether the potential attacks are feasible and how they might be prevented.

Assets

Mobility
Equipment (Relay equipment, HTs, vehicular)
Frequencies
Codes being used
Information being carried
- *Driver's license number*
- Criminal record
- Address
- Credit card numbers

Secret operations
Tower
Antennas
Receiver
Lives of public service personnel
Ability to communicate important information in a timely manner
Actual communications transaction
Location of activity/event
Availability of communications link
Physical infrastructure – towers, radios, antennae
Bandwidth
First responder's lives
DB of private information (e.g., NCIC)
Property and lives of citizens to be protected

Listed above are a set of assets identified by other sections of this class. Not attempt has been made to filter or sort the concepts, so there may be redundancy between the different groups. Items in italics are those that were considered to be especially important.

Perpetrators

Drug dealers
Criminals (organized crime)
Ham radio operators
Media
Teenagers
Spys
Lawyers
Terrorists
Thrill seekers
Curious listeners
Nature
Equipment vendors
Taxi drivers
(Foreign governments)
Curious listeners
Personal rivals
Disgruntled employees/officers
The media
Hackers
Accidental interferers
Service/equipment provider
Competitor

Threats

Listening
Inserting false information/transmission
Steal BW
Physical destruction of infrastructure
Try to access private information/DB
listen to police call and get to scene of accident/crime and interfere with operations
Exposure of sensitive people or operations (e.g., undercover)
Disruption of prosecution or other long-term operation
Perpetrator learns frequency of operation and then jams/intercepts
Public discovery and access to location of operation/event
Natural disaster, failures
Terrorist attack
Power failure
Jam link
- ***By accident***
- ***For fun***
- ***For profit (e.g., rob bank and prevent response)***

Intercept vehicles
Broadcast false information
Arrive at scene, tamper with evidence
Theft (looting)
Create diversion
- verify its success

Put police, fire, EMS lives in danger
Exposure of private information thru media, damaging a case in progress
Blackmail
Commit crime
Cause damage to receiver (e.g., local EMP)
Identity theft
Cut down tower
Generate signal to cause intentional distortion to jam link
Disrupt/spoil ongoing operation or investigation
Eavesdropping
Steal bandwidth
Generate false transmissions to confuse
Tamper with signal
Rebroadcast over public broadcast radio
Make communications undependable

Existing Safeguards

Encryption
Codes
Proprietary radio systems, proprietary protocols
Hidden frequency of operation
Abitilty to direction-find transmitters
Transmitter generated ID code
Human safeguards:
- Procedures
- Codes
- Recognition of voices

Frequency hopping
Penalties/regulations
Sting operations and false operations to catch miscreants
Physical protection of facilities
Redundancy of facilities
Emergency hot spares

Password protection of DB access
Choice of modulation technique
Protection against jamming
Digital transmission
Legal sanctions/penalties
Management of system
Honeypots
Power control
OOB signaling
Control of equipment distribution
Backup system/facility
Battery or emergency power

Note: Some of these existing controls aren't actually existing controls, but are more additional controls.

Vulnerabilities

Scarce spectrum
Interference
Human error in operations
Spectrum is accessible anywhere
Link is accessible anywhere
RF technology and hacker technologies are widely available
Carelessness
Elevation of antenna/tower attracts lightning
Confusion of modulated signal with noise/interference
Inability to disguise location of transmitter
Known protocols
Leakage of operational information
Budget limitations
Inadequate penalties do not deter misbehavior
Immoral society
Lack of interoperability

Fixed frequency of operation.
Analog transmission
Mostly unencrypted
- voice (general operations)
- data (DB access)

generally accessible transmitter and other facilities
no central coordinatoion
interoperability
funding
limited spectrum
inadequate legal penalties
lack of enforcement of legal penalties
inteference
insufficient back up power
flawed software
homogeneous network
failure during system overload/catastrophe

Additional Controls

Profiling attackers
Beamforming
Intrusion detection
Software validation
System validation against security needs [*ASSESSMENT*]