Wireless Systems Security

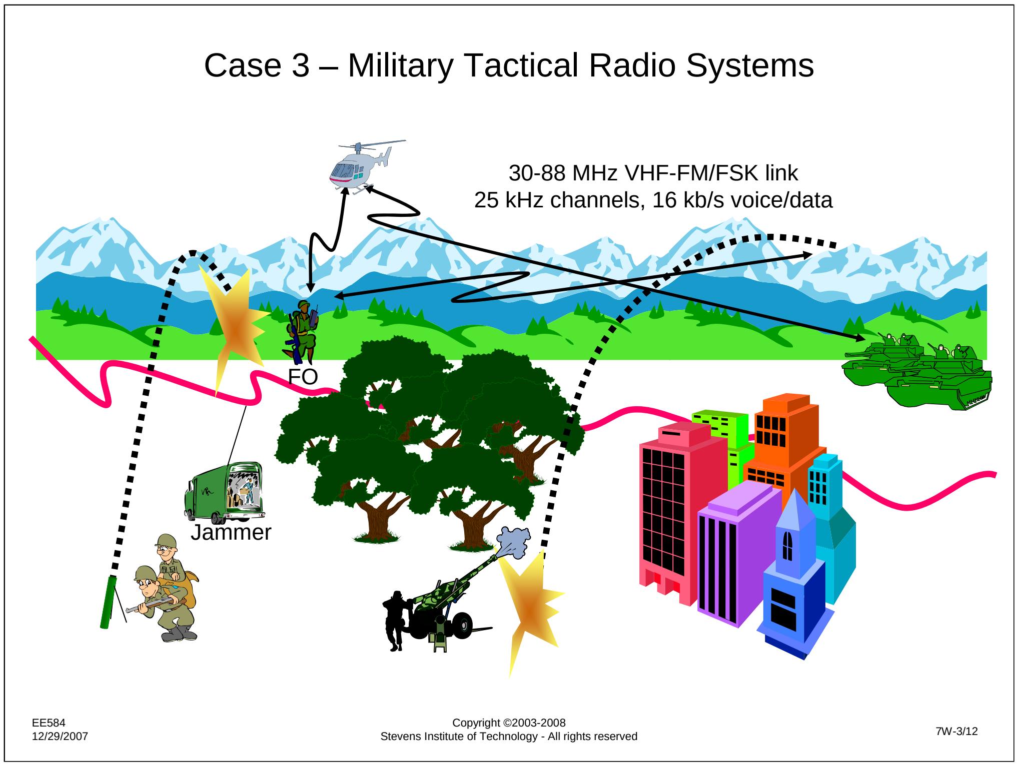
EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

Week 7 - Wrapup

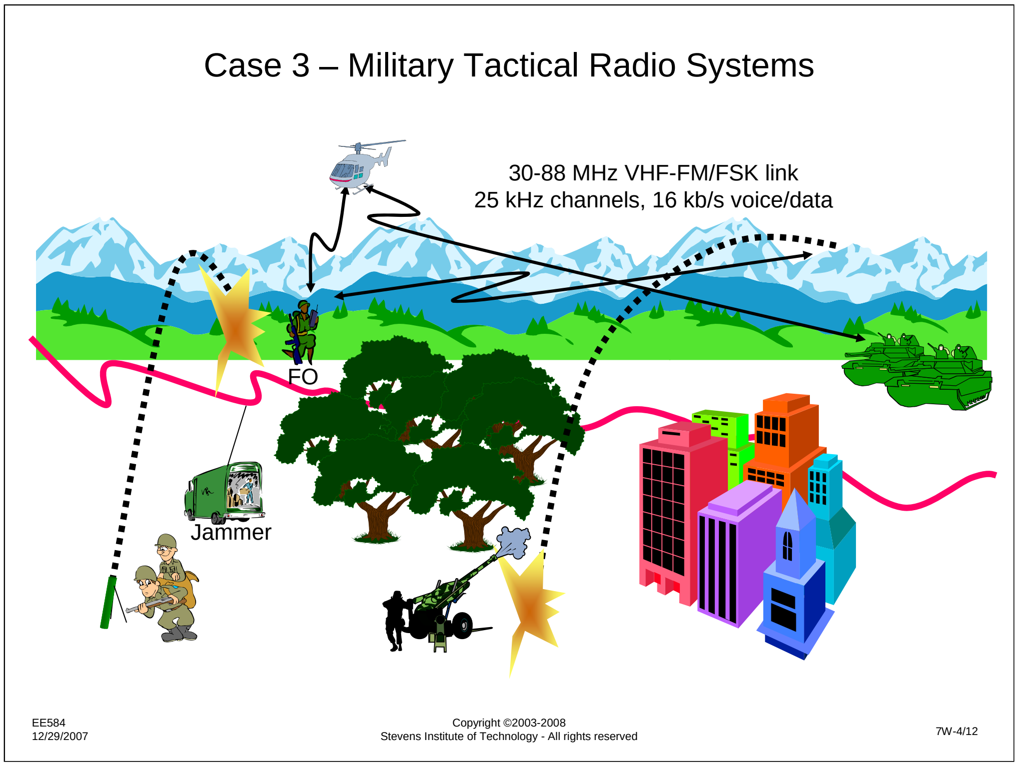
Case Study 3
Summary and observations

At this point, you have completed the discussions for the third 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.



I picked the military tactical radio system as the next case study for a particular reason. It is very similar to the public service wireless network in technology and, to a limited extent, in operation. However, there is a major difference in the threat environment. While the police and fire fighters have to deal sometimes with technilogically well-equipped and intelligent adversaries who are trying to cause them harm, for the most part, their operating environment is relatively benign. On the other hand, the military must assume an enemy who has essentially the same resources as they have and is willing to use any means necessary to deny them their goals. For this reason, the military communications systems have evolved to deal with the more stringent security requirements.

In past conflicts, threats like radio direction finding, jamming, interception, replay of prior transmissions, and intentional attempts to inject false messages in to the communications system have been used. Using technologies like encryption and electronic counter-countermeasures (ECCM) have evolved to protect the integrity, confidentiality and availability of the communications systems. In addition, procedural controls and operational doctrine are used to maximize the likelihood of correct operation in the presence of enemy operations.



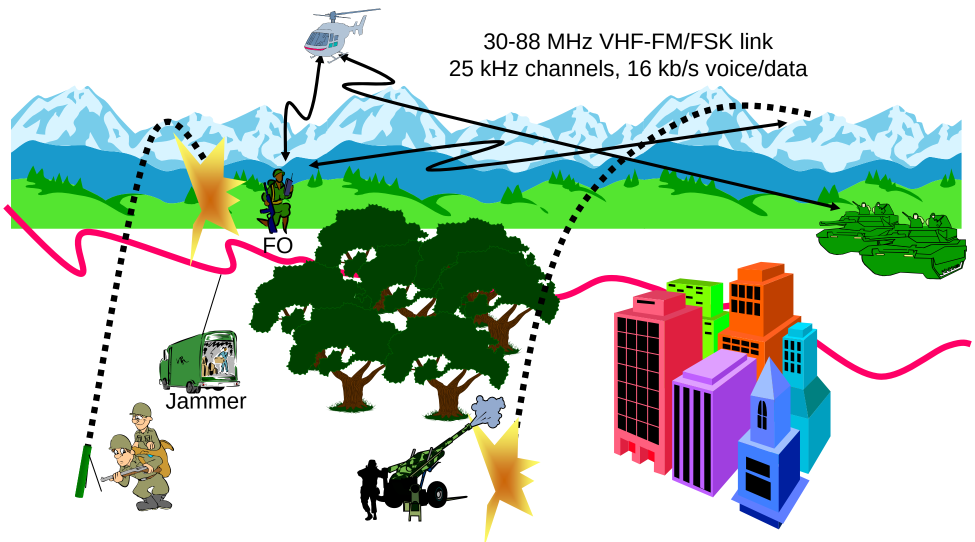
I'd like to focus on one aspect of operating in a hostile environment to illustrate an important technical concept, that of "circular error probability," (CEP).

Consider the game that is played between the FO and the enemies directing mortar fire at him. If they can locate him accurately, they should be able to quickly neutralize his effectiveness, by either killing him, destroying his equipment, or forcing him to flee. To be able to locate him, they have to engage in direction finding (DF'ing). If the signal they receive from the FO is strong, compared to the background noise, it should be easy to determine when they are pointing their DF'ing equipment at him. Alternatively, they can set up two antennas and examine the difference in the time of arrival of the FO's signal at the two antennas. If the SNR is good, it is easy to make an accurate time difference measurement. If the SNR is poor, the accuracy of the measurement will be degraded.

One measurement only indicates the direction of arrival of the signal. With at least two measurements from different locations, it is possible to identify the position where the two measurements intersect, determining the FO's position. Naturally, the more accurate and precise the two measurements are, the smaller the area identified where the FO is likely to be. This measure of the position accuracy, or actually, the probability that the FO is within a circle of a given radius, is the CEP. To minimize the number of mortar shells they need to fire to hit the FO, the enemy wants to minimize the circle area that defines the most likely position of the FO. Obviously, he would like that circle to be as large as possible. Decreasing the enemy's detection SNR is the best way to do this.

Since the FO must be transmitting a certain signal power to be able to reach the command post, reducing transmit power isn't an option. Using a directive antenna might help, but that is likely to visually compromise his position. The other option is to use a spreading code unknown to the enemy to make the effective SNR the enemy sees very low – ideally negative. This is the low probability of intercept (LPI) capability of spread spectrum.

Case 3 – Military Tactical Radio Systems

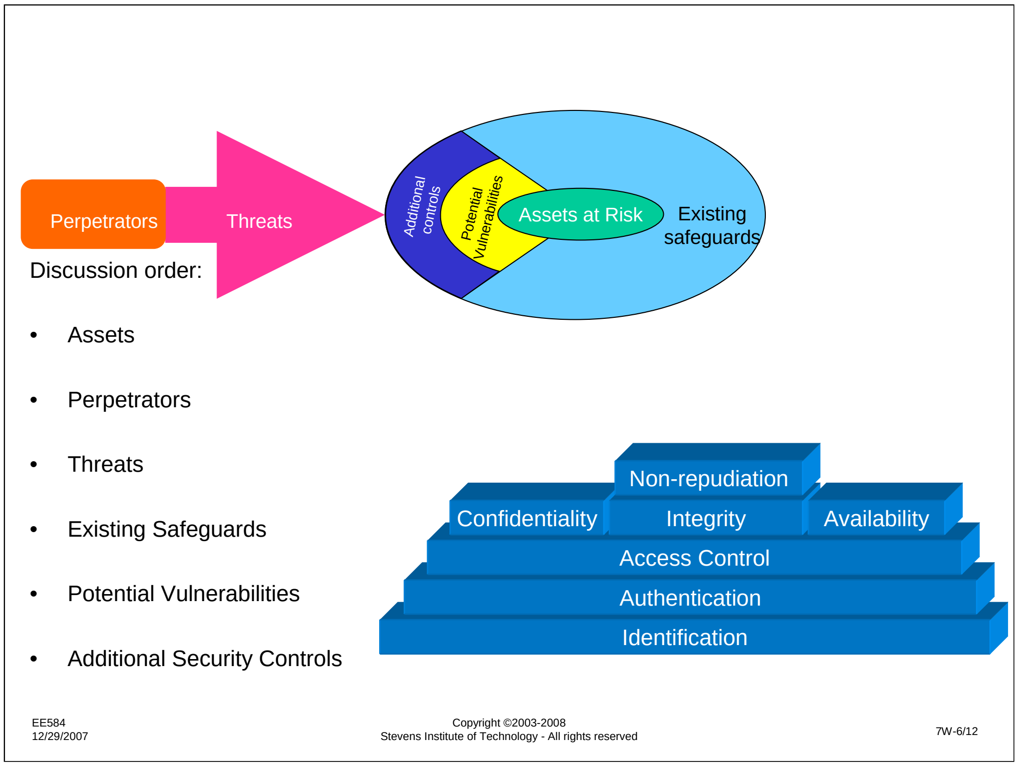


EE584
12/29/2007

7W-5/12

The use of security techniques like cryptography and ECCM offer a great deal of protection (integrity, confidentiality and availability) to the military users of these systems, but this creates a significant vulnerability – if a piece of equipment is captured by the enemy without the knowledge of the friendly forces, not only might their communications be compromised, but worse, they may continue to operate with the false sense of security that anything they send is protected. There are a number of documented cases where compromised enemy security technology was used very sparingly, even if it meant putting other assets at risk. (For instance, see “The Puzzle Palace” by James Bamford for a description of an Israeli attack on the US Liberty – a ship that was routinely monitoring their encrypted communications – including real-time intercepts that were decoded at NSA and indicated the attack was imminent.)

So, how do you use this valuable technology in the high-risk areas where it is needed most? There are three mechanisms to avoid or constrain compromise: (1) strict orders to the users that they must use all available means to destroy the devices if capture is expected, (2) easy to use controls that allow quick erasure of the most valuable information – the key variables that control cryptography or spread spectrum operation, and (3) procedures that routinely change the key variables, limiting compromise to, perhaps, the remainder of the day when the device is compromised. In addition, by providing a means for the user to install the day’s key variable without direct knowledge of the value, the risk of forcing the user to reveal the information is eliminated.



You have now seen both sides of the security assessment process and hopefully you appreciate that it is easier to think about attacking a system than it is to defend it. I am reminded of a saying that comes up when people are commenting on the work of others – "It is easier to criticize than to create." The defender has to be in the role of a creator, inventing ways to defend the system against all feasible attacks, while the attacker only has to find one hole.

Again, the focus on system attacks, even by the defender, helps to understand the issues that might exist.

Assets

- Equipment
  - Crypto key
- Soldier's life
- Operations
  - Frequencies
  - Procedures
- Equipment shelters
- Command center
- Information transmitted
- Other physical assets (tanks, vehicles)
- Outcome of engagement
  - And therefore national security and ultimately freedom
- Codes, security procedures
- Tactical advantage
  - Surprise
  - System technologies
- System design
- Perceived strengths (2-ways)
- Fear factor

- Communications bandwidth
- Operating frequency
  - hopping pattern
  - DSSS – spreading sequence
- Crypto
- ECCM
- ***Command center – and location***
- Forward Observer – and location
- All communications system elements
- ***All soldiers lives***
- ***Vehicles, aircraft, weapons, artillery***
- ***Power***
- ***Voice/data content***
- Tactical advantage
- Traffic flow/load

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

Spy
Enemy
Traitor
Double agent
Terrorists
Nature
Foreign government
Fun seeking hackers
Thieves
Black market
Organized crime
Russian mob
FMP'ed AT&T employees
EE/TM584 students looking for more income
Program competitors

Enemy – intel, jammer operators, direction finder operators
Turncoat/traitor
Enemy supporters
Press
Terrorists
Equipment competitors

Threats

Jamming
Spoofing – fraudulent information
DF'ing – bearing and distance
    To attack location
    To track movements
Destroy radio link
Kill the FO
Detecting transmitted information
"Friendly" disclosure of information
Inclement weather
Damage to equipment
    Lightning strike
    Driven over by tank
    Bombed
    Exploding battery
Exploit knowledge of POWs about system, operational procedures
Exploit designers
EMP
Replay transmissions

Jamming
Interception
Kill the Forward Observer
Physical destruction of equipment
Cause waste of power
Observe connectivity
observe traffic flow
    to identify operations
    to identify command structure
Spoofing/replay
Traitor sells: content, keys, eccm settings, operation al plan
Equipment manu sells info, equipment
Exposure of operational data that compromises location
Upload virus to CC computer
Attacker tries to steal /compromise crypto/keys
Stealing bandwidth
Enemy attacks communication link to cause segmentation of communication network
Enemy captures radio and operations on network

Existing Safeguards

Air superiority
Technical advantage
Hiding equipment in trees
Crypto
Frequency range limits accessibility to signal due to propagation
Encryption
Frequency hopping
Antijam – Direct Sequence Spread Spectrum
EMP protection
No tone squelch
Access to wide variety of data, etc., services
Physical construction of radio
Training/intelligence of operator

Crypto/ECCM – zeroize
FH
DSSS
Crypto
Power control
Physical security protecting radio operator, Forward Observer

EE584
12/29/2007

7W-10/12

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

Vulnerabilities

- Wireless nature of system
- Potential for interference
- Finite fuel source – battery
- Portable
- Fixed design elements
  - Protocol
  - Crypto algorithms
- Human operators – human error, wrong mode of operation
- Frequency range is limited
- Physical construction – fragility
- Operating environment
  - Heat
  - Sand
  - Rain/water
- Budget restrictions
- System complexity leads to systems failures
- Loss of power
- Lack of environmental controls
- Design flaws
- Misconfiguration
- Size/weight of equipment
- Battery power
- Exploding batteries
- Centralize C3 structure
- No user authorization on communications link
- Broadcast, not addressable radio

Additional Controls

Augment batteries with solar power
Remote maintenance
Software defined radio
Biometric user ID
Self-destruct (zeroize)
Peace
Position reporting capability to track captured systems
Physical hiding/protection of equipment
Sprint picture phone
Beamforming/smart antennas