Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

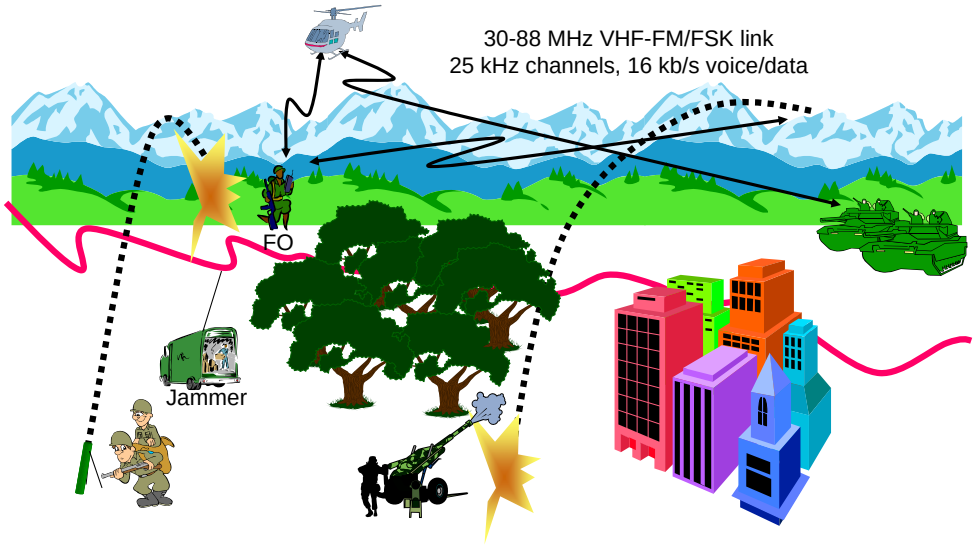
Week 7

Case Study 3

This week we will address the third case study. As it was for last week, you should discuss the security issues in the WebCT discussion groups I have set up. These are labeled Red Team 3 and Blue Team 3. DO NOT POST THIS WEEK'S DISCUSSION TO THE TEAM 2 GROUPS. It may not be read by other students and will certainly be confusing.

This week, I switched the teams – if you were on a Red team last week, you are on a Blue team this week, and vice versa. In future weeks, I will randomize the team assignments.

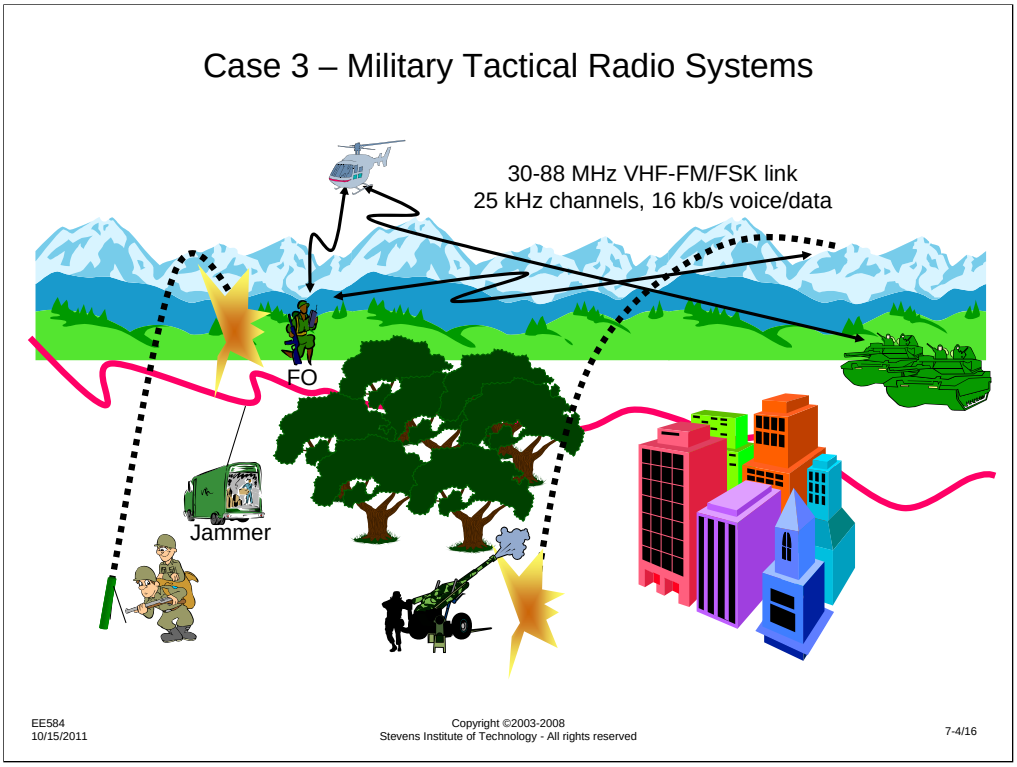
Case 3 – Military Tactical Radio Systems



EE584
10/15/2011

7-3/16

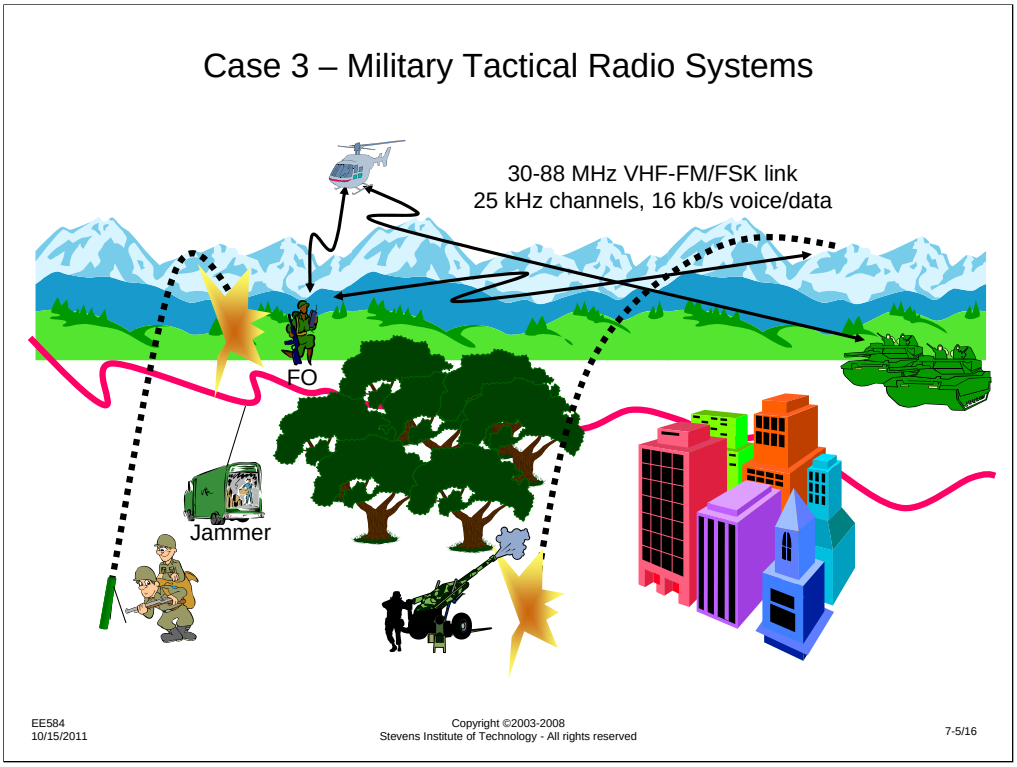
This week's assessment deals with military tactical radio systems. The system architecture and the environment is somewhat dated – I am describing the system as it existed during the Cold War, where the USSR was the enemy and had comparable technical prowess to the US. However, the important point is that the military systems were designed with security in mind from the start. Although they have traditionally operated in the same frequency range as the public service wireless systems, and have traditionally used the same modulation technique (VHF-FM systems), the significant difference is the recognition of the severe threats to the systems. Specifically, I am describing the SINCGARS (Single Channel Ground Airborne Radio System) as it was originally envisioned in the 1970s – 1980s. It is significant to realize that 20+ years later, the same hardware is in use, due to the long lifecycle of military systems. It is this long lifecycle that makes the designer consider how the system has to be protected today to deal with the threat that is likely to exist a quarter of a century later.



During the Cold War, it was generally assumed that World War III would be a conflict between the United States and the Soviet Union. The typical scenario was that the war would start as the USSR invaded Eastern Europe in a conventional war, unlike the terrorist attacks and guerrilla war we see today.

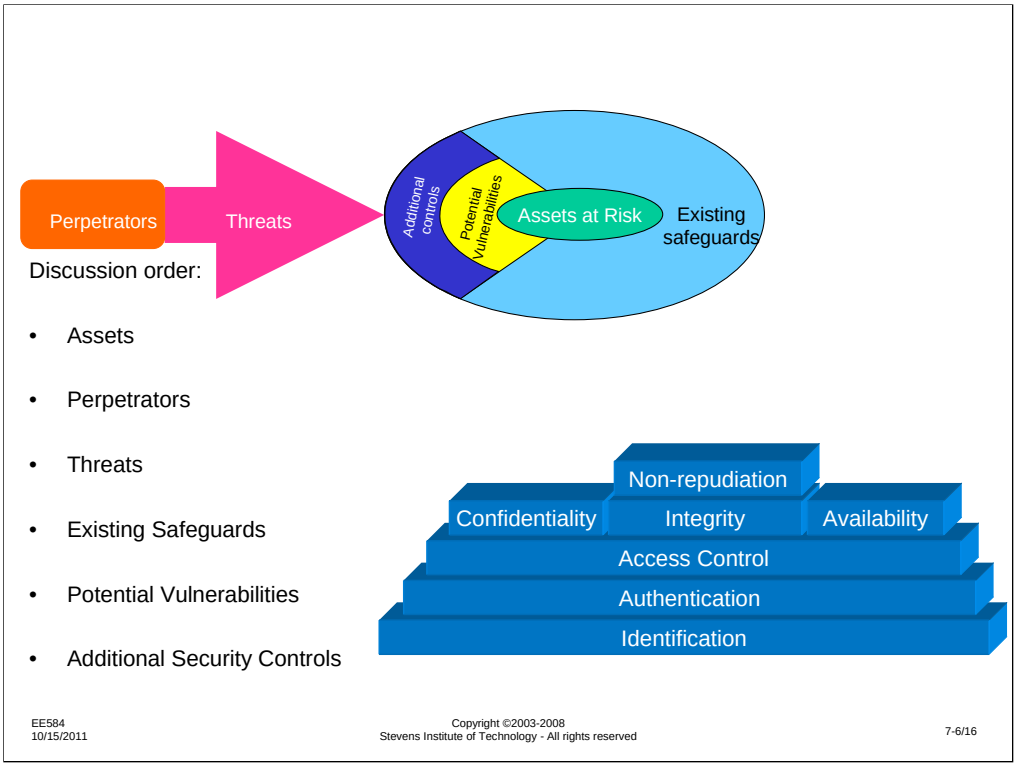
In conventional warfare, there is typically a battle front or a “front” where the most intense fighting occurs. This boundary between the good guys and the bad guys, shown as a red line in the diagram above, demarcates the sides and the area around has been referred to as the FEBA – Front Edge of the Battle Area. In conventional warfare, heavy artillery would be located a long distance from the FEBA, illustrated as firing from behind the mountains in the distance on the right. As the enemy areas (the bottom of the illustration) are controlled, mechanized infantry, tanks, and other assets would be brought in.

To coordinate the advance of the attack, a “forward observer” or FO would often be placed very close to the enemy forces. They could spot the enemy positions and communicate them back to the artillery and other forces well away from the current activity. Obviously, the enemy would like to avoid giving the attacking forces the advantage of a spotter, so they would try to eliminate the threat to their activities created by the FO. Thus, he is likely to be a high priority target, shown by the mortar fire at the left side of the slide.



This placement of communications links leads to a couple of interesting characteristics. First, the FO is very close to the enemy positions, but far from his headquarters. If he transmits with enough power to reach the headquarters reliably, he may give away his position to the enemy. This leads to the requirement for "LPI" – Low Probability of Intercept. By using spread spectrum technology (similar to CDMA), the FO can transmit a signal that is easily decodable by friendly forces, but is undetectable to the nearby enemy. In addition, since the FO is close to the enemy position, he is subject to being jammed. The headquarters transmission that is asking for the coordinates to send artillery may need to travel 30 km, while the enemy jammer is 5 km away. This distance difference makes the energy from the jammer much stronger than the desired signal from headquarters. Again, the CDMA-like spread spectrum technology can provide AJ (antijam) protection. Since the jammer does not know how the desired signal has been scrambled, they cannot jam effectively. Using spread spectrum to smear the signal over, for instance, a 3 MHz bandwidth, compared to the, perhaps, 30 kHz that the transmission actually requires would provide a 20 dB (10*log(3,000,000/30,000)) advantage.

With the generation of tactical radio systems that was used before SINCGARS in Viet Nam, it became clear that monitoring, replaying transmissions, and other means of attack were serious issues. For this reason, very high security cryptographic systems were made an essential part of the tactical military radio systems. Although cryptographic hardware translates into more weight, more power consumption, and higher cost, all important issues for a system that would be carried by soldiers in battle and would be widely deployed, the goal of being able to secure 100% of the radio transmissions was an important one.



As for the last assessment, if you have been assigned to a Red Team, you should be concentrating on the following items:

Assets: What is it about the system that you would be interested in stealing, destroying, disrupting, etc.?

Perpetrators: Who are you? Why do you do the evil things you do? Who is backing you, or what resources are available to you?

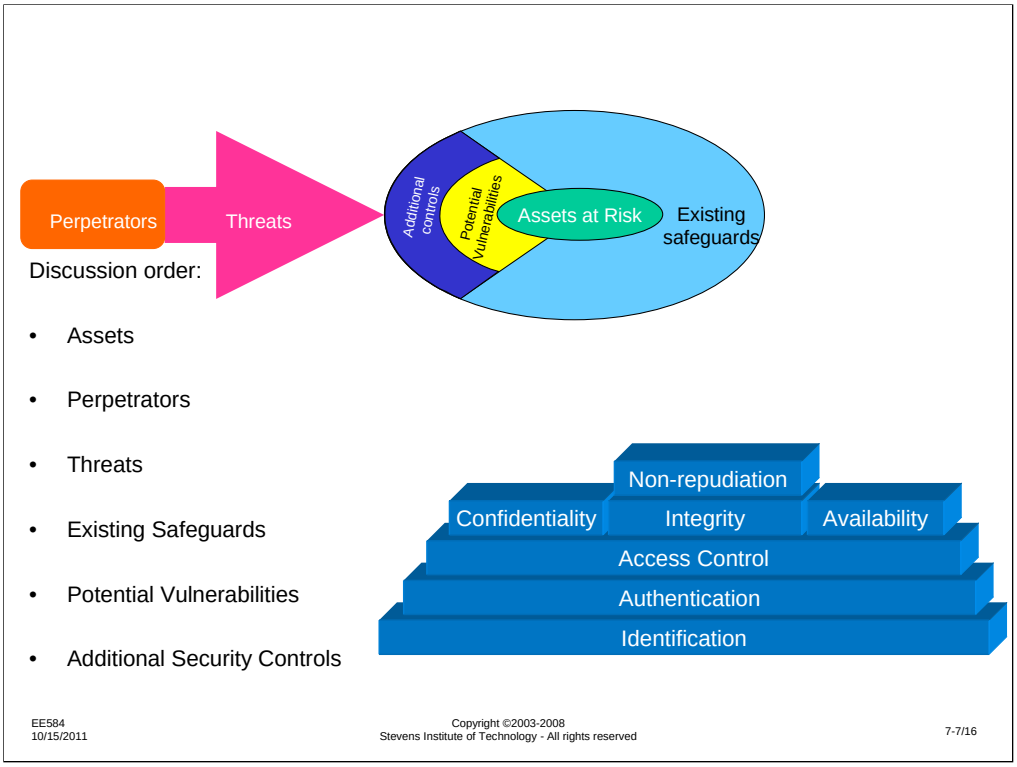
Threats: What mischief can you get into? How would you do it?

Safeguards: What are the things that are, or might be, in your way?

Vulnerabilities: What unlocked doors, open windows, unprotected ways in might exist?

Additional Controls: What might the defender do to make you life harder?

Keep in mind the security architecture at the bottom right. For each security service, there might be something that you can do, steal, break, etc.



Likewise, if you have been assigned to a Blue Team, you should be concentrating on the following items:

Assets: What is valuable to you in your system? What might the attacker be after?

Perpetrators: Who should you be on the lookout for? How do they operate? What are they capable of?

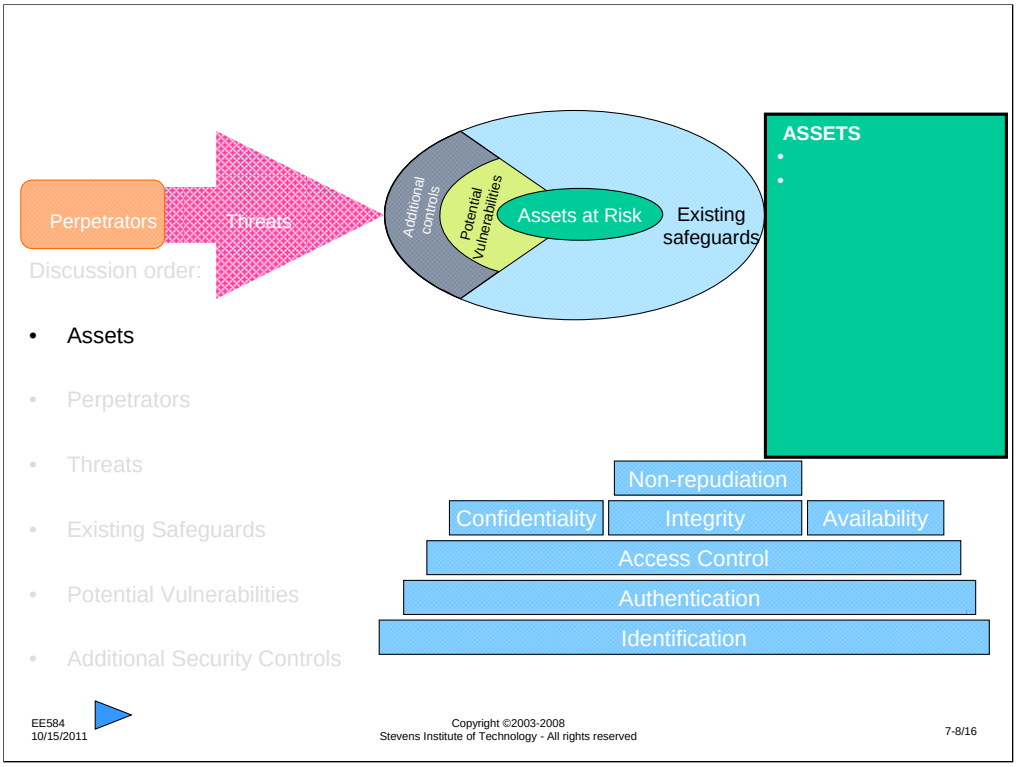
Threats: How might someone try to attack your system?

Safeguards: What protection is already in place?

Vulnerabilities: What might have been missed? Where are they most likely to try to enter?

Additional Controls: How could you make the system stronger? Would it be worth it?

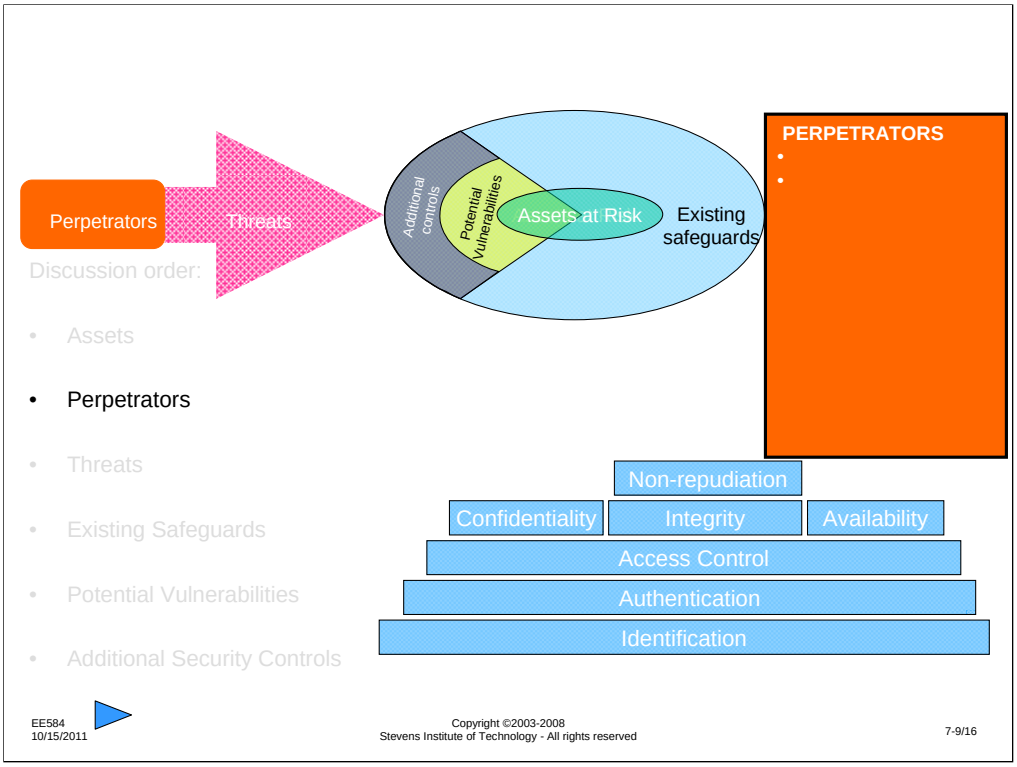
Keep in mind the security architecture at the bottom right. For each security service, there might be something in your system that needs protecting.

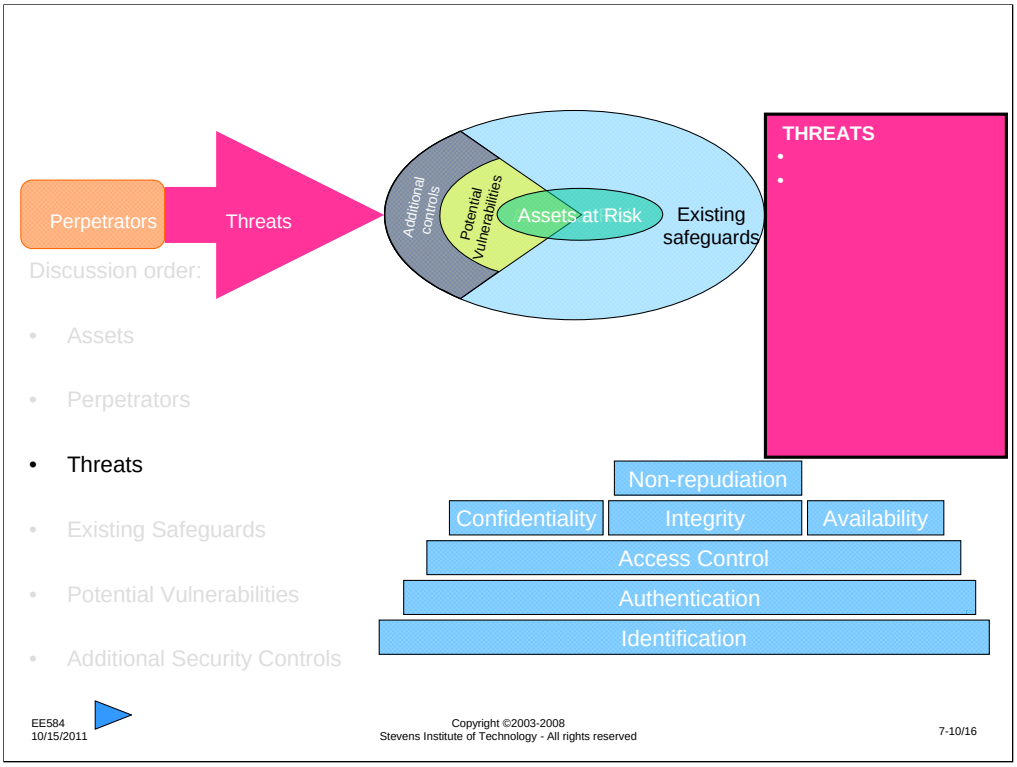


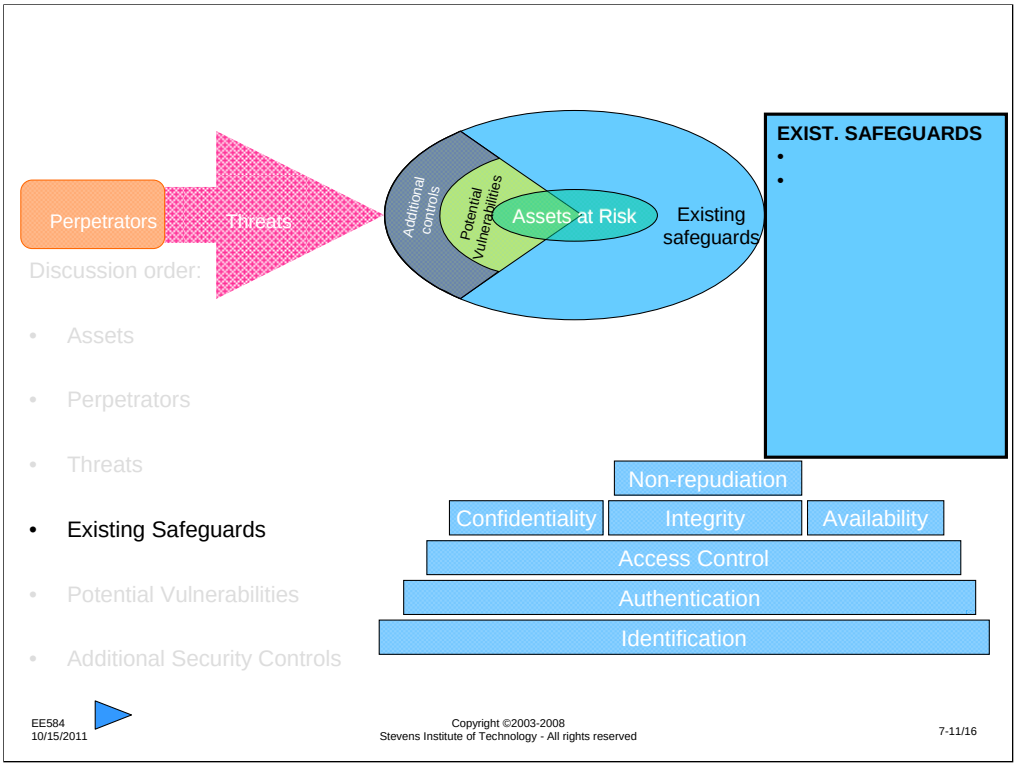
Again, I recommend that as you examine the system under discussion, you create a discussion topic for each aspect of security and/or for each element of the security assessment process. This is a brainstorming process, so don't worry about silly suggestions or things that are not in the right discussion thread. Post as many ideas as you can think of and respond to the postings of others with more ideas.

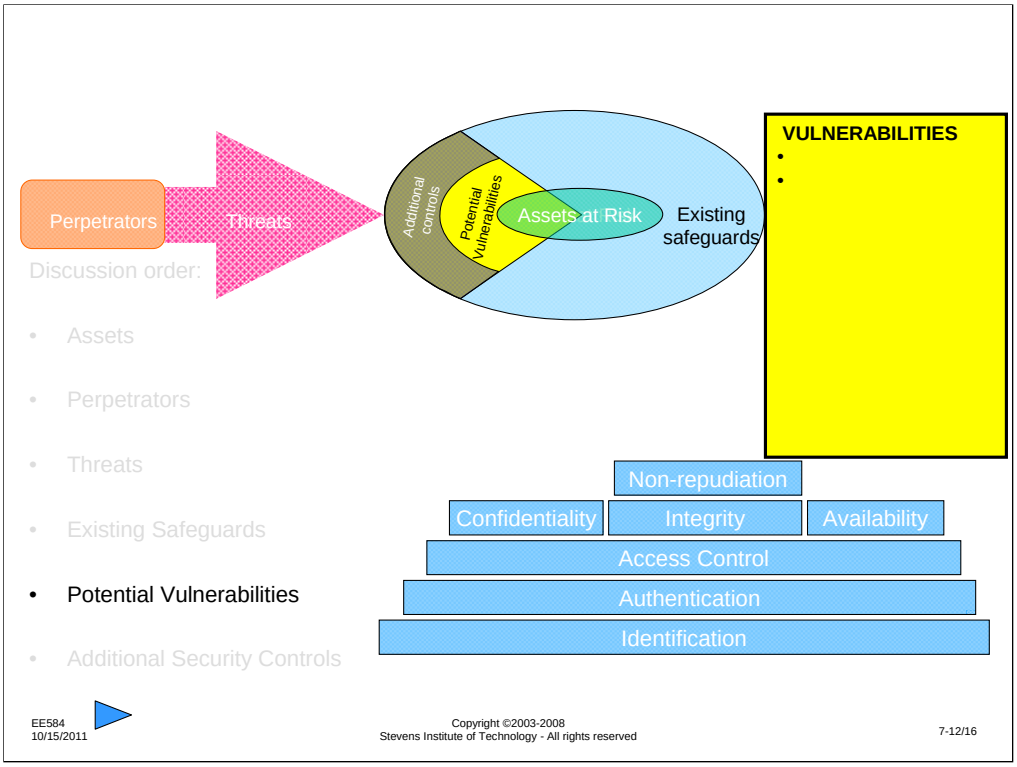
The Red Team will not be able to see the postings of the Blue Team during this week and vice versa. Next week, both sets of discussions will be open to the other group. I encourage each group to compare their thought process with the process of the other group. You can, however, look at last week's assessment discussions. In addition, I will have posted summaries of assessments that were performed on last week's topic by previous sessions of this course so you can compare your group's assessment to previous ones. There will be some common items, but I am sure there will be some that one session or the other did not encounter. As this course is repeated, I expect that the cumulative assessment discussion will converge to a common set of issues.

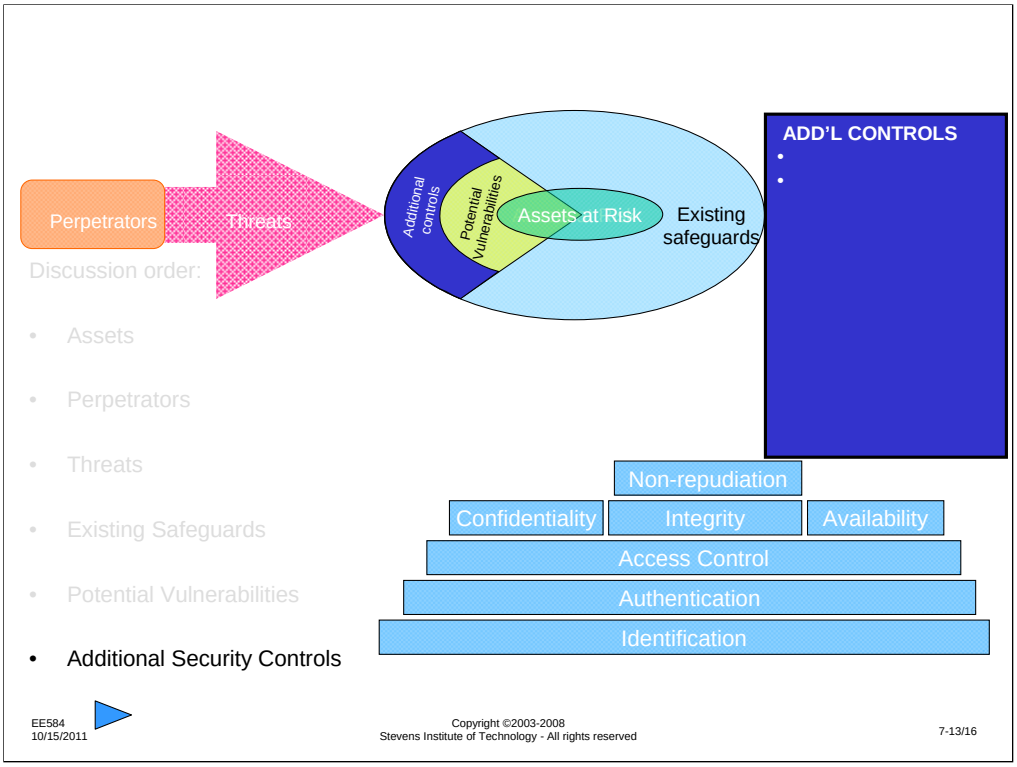
Next week, we will begin another assessment on another system. At that time, again, I will summarize the discussions and will add some more information about issues in the system that may not have been addressed.

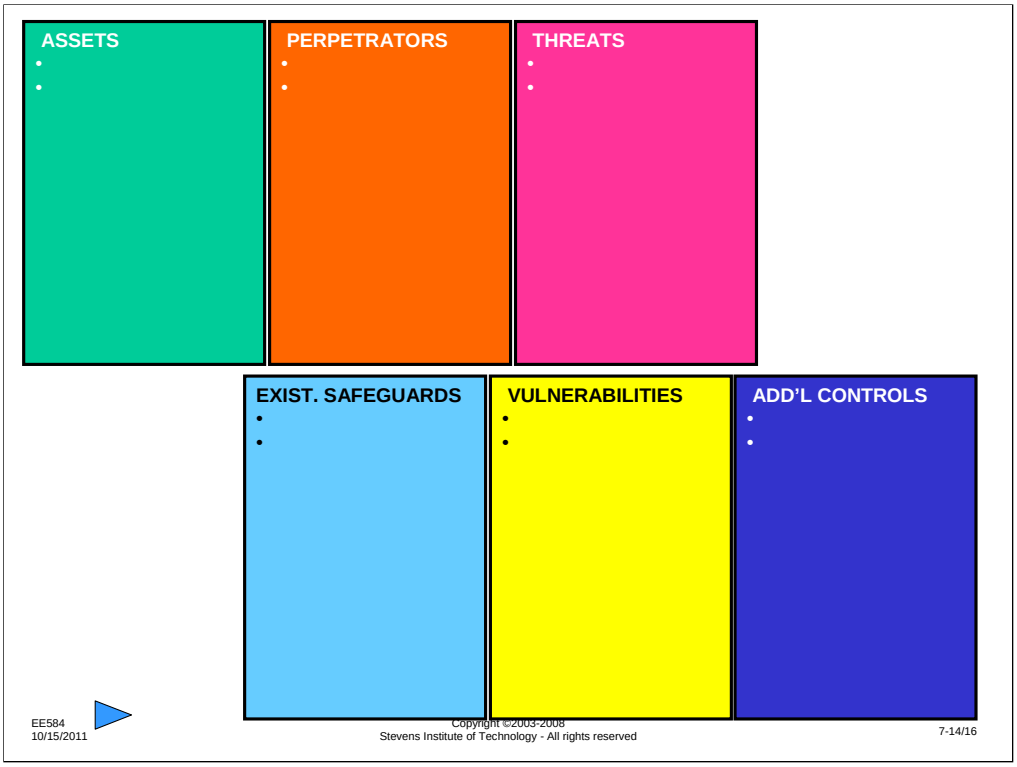

Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards
PERPETRATORS
Discussion order:
Assets
Perpetrators
Threats
Existing Safeguards
Potential Vulnerabilities
Additional Security Controls
Non-repudiation
Confidentiality
Integrity
Availability
Access Control
Authentication
Identification
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-9/16


Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards
THREATS
Discussion order:
• Assets
• Perpetrators
• Threats
• Existing Safeguards
• Potential Vulnerabilities
• Additional Security Controls
Non-repudiation
Confidentiality
Integrity
Availability
Access Control
Authentication
Identification
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-10/16

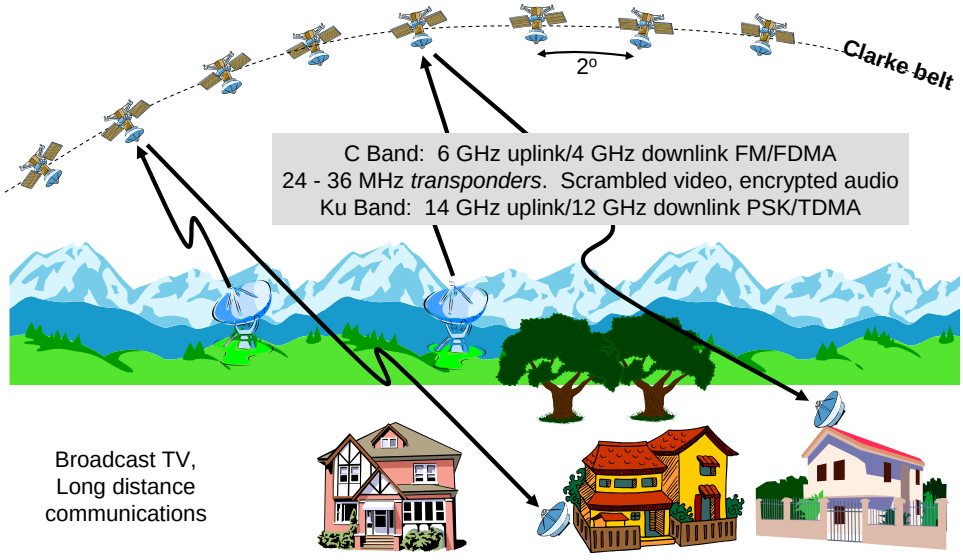

Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards
EXIST. SAFEGUARDS
•
•
Discussion order:
• Assets
• Perpetrators
• Threats
• Existing Safeguards
• Potential Vulnerabilities
• Additional Security Controls
Non-repudiation
Confidentiality
Integrity
Availability
Access Control
Authentication
Identification
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-11/16


Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards
VULNERABILITIES
Discussion order:
Assets
Perpetrators
Threats
Existing Safeguards
Potential Vulnerabilities
Additional Security Controls
Non-repudiation
Confidentiality
Integrity
Availability
Access Control
Authentication
Identification
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-12/16


Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards
ADD'L CONTROLS
Discussion order:
Assets
Perpetrators
Threats
Existing Safeguards
Potential Vulnerabilities
Additional Security Controls
Non-repudiation
Confidentiality
Integrity
Availability
Access Control
Authentication
Identification
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-13/16


ASSETS
PERPETRATORS
THREATS
EXIST. SAFEGUARDS
VULNERABILITIES
ADD'L CONTROLS
EE584
10/15/2011
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
7-14/16

Case 4 – Satellite Communications Systems



Next week's assessment will deal with satellite communications system. Research some of the applications of satellite communications and the technology involved for next week's assessment. Entertainment services are some of the biggest applications of satellite communications – news uplinks, TV backhaul for network television distribution, satellite radio, etc. are some of the more popular applications. In the past, long distance telephone communications were frequently transmitted using satellite links, but have been mostly replaced by long distance fiber optic systems.

Course Project

- Pick a topic you are interested in or project you may be working on. Topic should involve either
  - A wireless system that has notable security issues
  - Security issues that are exacerbated in wireless systems
- Research the topic – current technical journal and conference paper references are desirable, but all sources are welcome.
- Prepare a 5-8 paper on the topic – due during the next to last week of class
- Prepare a short presentation on the topic – due during the next to last week of class
- Material covered in paper should address:
  - Background on topic: What is the general issue being addressed?
  - A brief assessment of the security aspects (use the structure of security assessments we have done in class)
  - In the context of the security services presented, what are the major security issues?
  - How dramatic are the security concerns (e.g., likelihood of attack)
  - Does it appear that there are efficient ways to improve security (e.g., cost-benefit tradeoffs)
  - What conclusions can you draw about the future directions for this topic (e.g., will it take major loss of assets to cause action to be taken? Is future technology likely to make the issue better or worse? How widespread is understanding of the underlying concern? What might change this? Is this a chronic or an acute issue?)
  - References
- The presentation should briefly cover the key points in the paper and provide detail on one or two

So far, there have been two papers assigned in the class. There will be a third that is due before the class project. The development of the papers' topics is: wireless technology, security technology, wireless security technology. The sources for the first two papers has been restricted to particular journals and conference proceedings. The third paper will be less restricted. In contrast, the project is completely open to any source you are interested in. The requirement is that the project deal with security in a wireless system.

Unlike the three papers, which are intended to be reviews of subject material, the project is intended to apply the security assessment methodology we have been discussing in the course. At this point, we will have completed three assessments with four more to do, each treating a different type of wireless system. Your project can either go into additional depth on a case study we have addressed, or can address a different type of system, as long as it is wireless and has security issues associated with it.

The project is in two parts. A 5-8 page written report, which I will not distribute to the class, and a "presentation" which will be shared with everyone. When I ran this course last semester as a live class, the presentations were the standard viewgraph presentation that my course slides would be in a live course. For this on-line session of the course, I would like you to prepare slides, but the slides should be accompanied by speakers notes, as I have annotated my slides. The audience should be able to look at the slides and read your notes to get the same information you would have presented if you were speaking in front of them. You don't have to, but if you would like to use the "Record Narration" feature of PowerPoint (in PowerPoint2000, this is a menu item under Slide Show), you may do so.

I need each set of slides, either in PowerPoint (NOT PowerPoint XP format – I can't open it), or Adobe PDF, or some other format you clear with me in advance, during Week 12 so I can put them up on WebCT during Week 13.

Note: It goes without saying that the presentation and the written project are ***ON THE SAME SUBJECT***. I have had students change their mind after they submitted the presentation, deciding that they couldn't find enough material to do the report. This suggests that they didn't start the report until the very last minute, despite the fact that this is supposed to be a term project. I will not accept a report that covers a different subject than the presentation.