

Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-1/15

Week 6

Case Study 2

EE584
12/29/2007

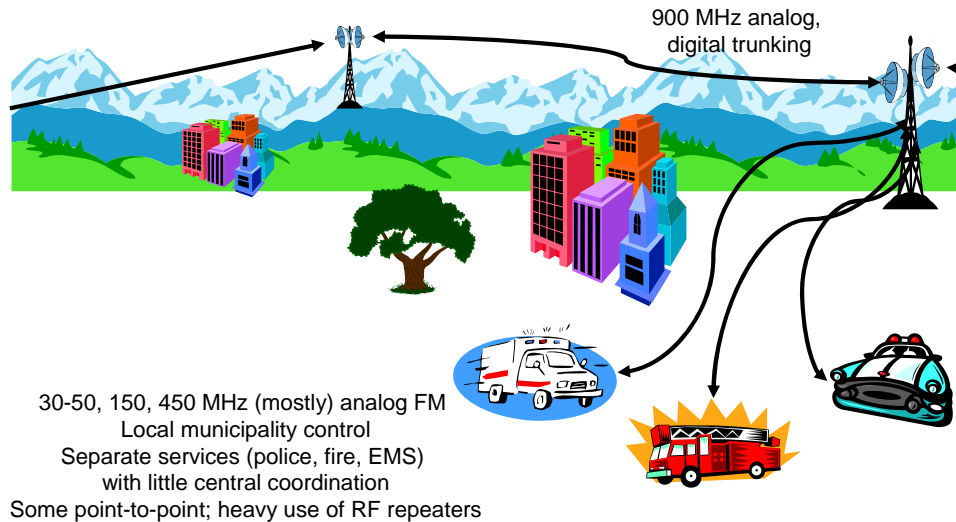
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-2/15

This is the first case study we will be going through in the course without the instructor providing the “answers” to the security issues up front. I encourage the class to interact throughout the week discussing the security issues in this system. When we have done this in a classroom setting, the discussion led to a lot of good observations from the students about potential issues. Instead of interacting during the class time, in this on-line version of the course, I will be providing my input at the end of the case study – next weekend.

Remember that participation in the assessment discussions are a portion of the class grade. I have done this to make sure everyone puts in their comments. Remember, that the process we are using is a brainstorming session, so there can never be a wrong answer or silly comment. The free flow of ideas is the only way to get to the real possibilities.

Case 2 – Public Safety Wireless Networks



EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

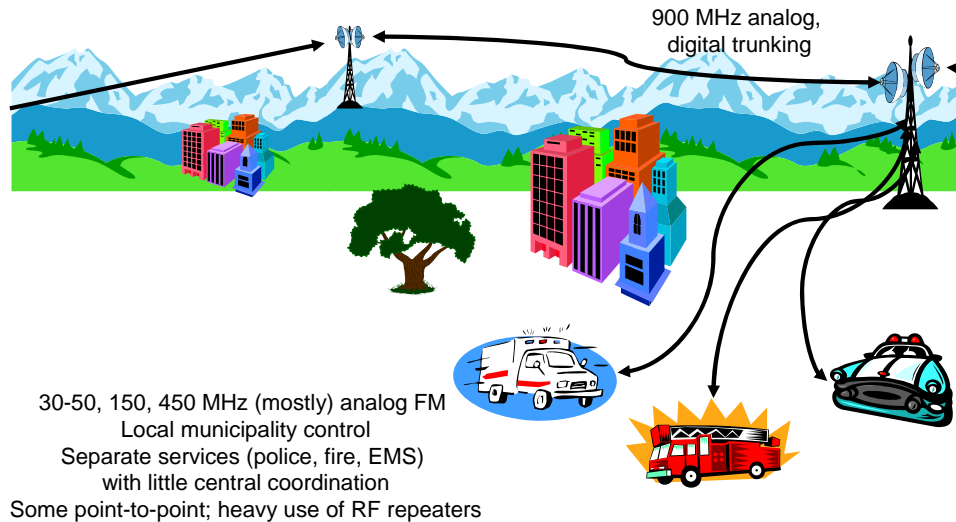
6-3/15

This assessment deals with the so-called Public Safety Wireless Networks. Police, Fire Department, Emergency Medical Services, etc., use these system for dispatch and the typical command and control processes.

For the most part, these systems use analog FM communications much the same as MTS, AMPS and ham radio VHF/UHF repeaters. In fact, in many respects, the contemporary systems are not significantly different than the system used by the Detroit police ~80 years ago. As RF technology has advanced and spectrum has become more crowded, these systems have moved from (first) 30-50 MHz, then to 150 MHz, and most recently to 450 MHz. Since most municipalities control their own law enforcement and safety organizations, the systems are often managed and deployed on a town-by-town basis. Further, since police, fire and EMS are generally separate organizations within a town, it is not unusual for the connection between their communications systems to be sparse.

For state-wide networks, e.g., the New Jersey State Police, the local (typically) analog FM systems are tied together through a backbone network, sometimes referred to as a "trunking" system. These systems have traditionally been analog 900 MHz point-to-point systems with recent movement to digital systems.

Case 2 – Public Safety Wireless Networks



EE584
12/29/2007

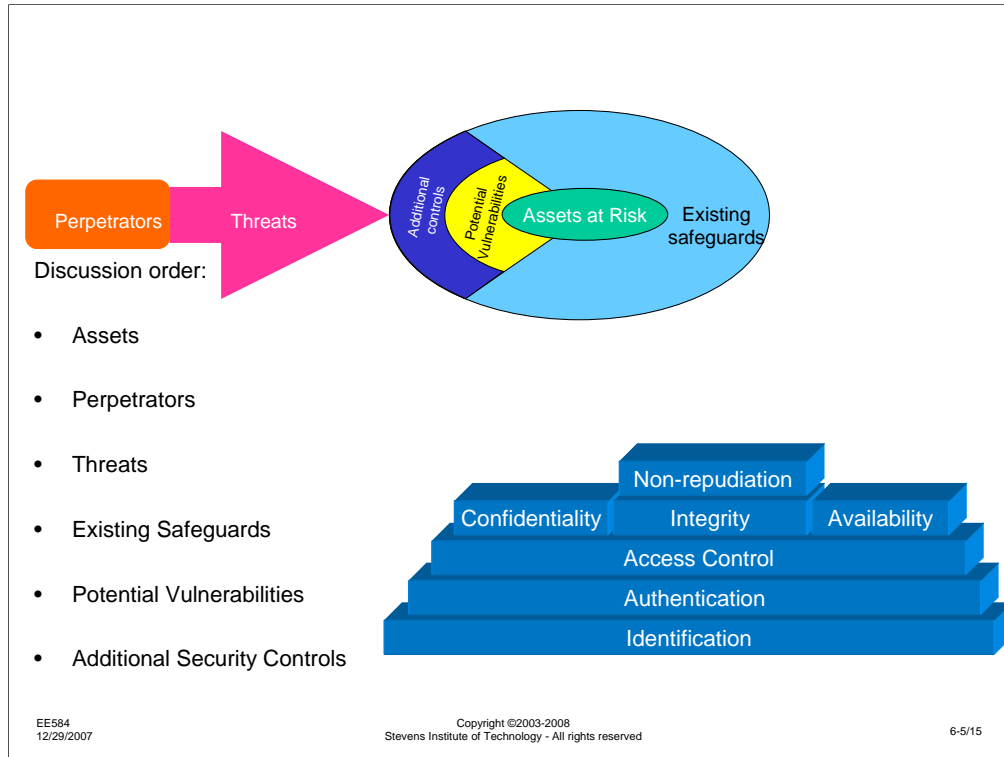
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-4/15

One of the side-effects of the distributed management and control of these public safety systems has been a lack of interoperability. Two near-by towns will often be operating on different frequencies, making it difficult to manage inter-municipality activities. For instance, an example that was presented by the New Jersey Office of the Attorney General (to whom the NJ State Police report) is this: a carjacking occurs in Newark; the thieves flee down US Highway 1, which passes through multiple cities and counties. Each town along the route attempts to intercept the stolen car, but must hand off to the next town at their border. While they may be able to communicate with the immediately adjacent town, it is unlikely that they can directly communicate with the second or third town away.

Another example exists in big cities and was highlighted on 9/11/01. A city like New York is so large that their individual department (police, fire, etc.) are large entities in their own right. While they may coordinate city-wide within the Fire Department, it is often the case that the police and fire fighters are completely independent. This was demonstrated on the morning of 9/11 when a police helicopter was circling the World Trade Center, observing the extent of the damage to the buildings. Although they recommended immediate evacuation of the building, this information could not be directly communicated to the fire fighters who were in the building, since their systems were incompatible. This problem obviously got worse during the search and rescue operations over the next several days when police, fire fighters and military personnel from the rest of the country came to assist. It is not unusual for a police car or fire engine to have numerous individual radios – one to talk to each of the other services in their town, and one to talk to each adjacent town.

Finally, there is the issue of capacity and spectral efficiency. As towns grow and require more municipal infrastructure communications, the available frequency allocations are heavily burdened. At the same time, the public services systems are operated more like the pre-cellular MTS system, with much lower spectral efficiency.



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?

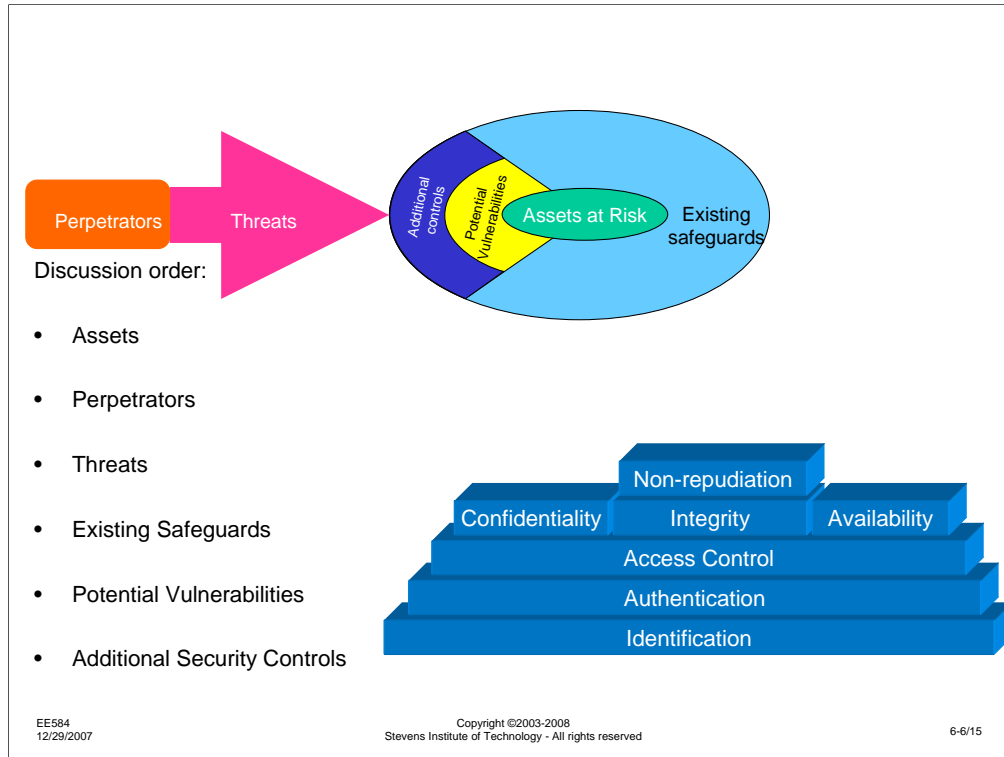
Threats: What mischief can you get into? How would you do it?

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 your 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.



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?

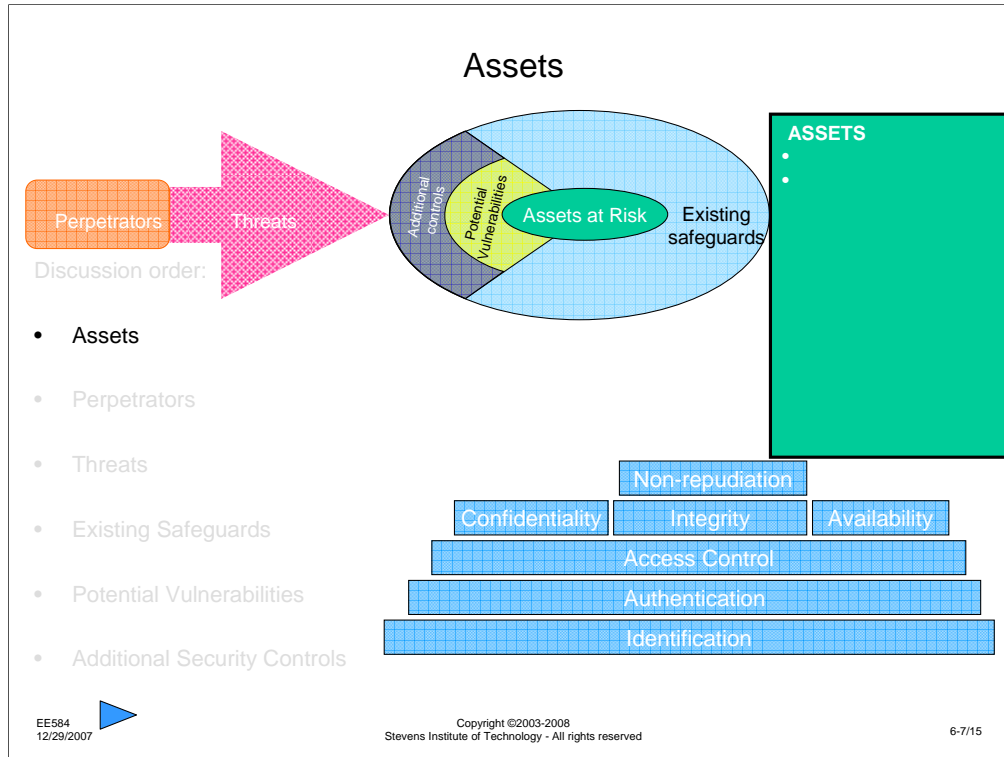
Threats: How might someone try to attack your system?

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?

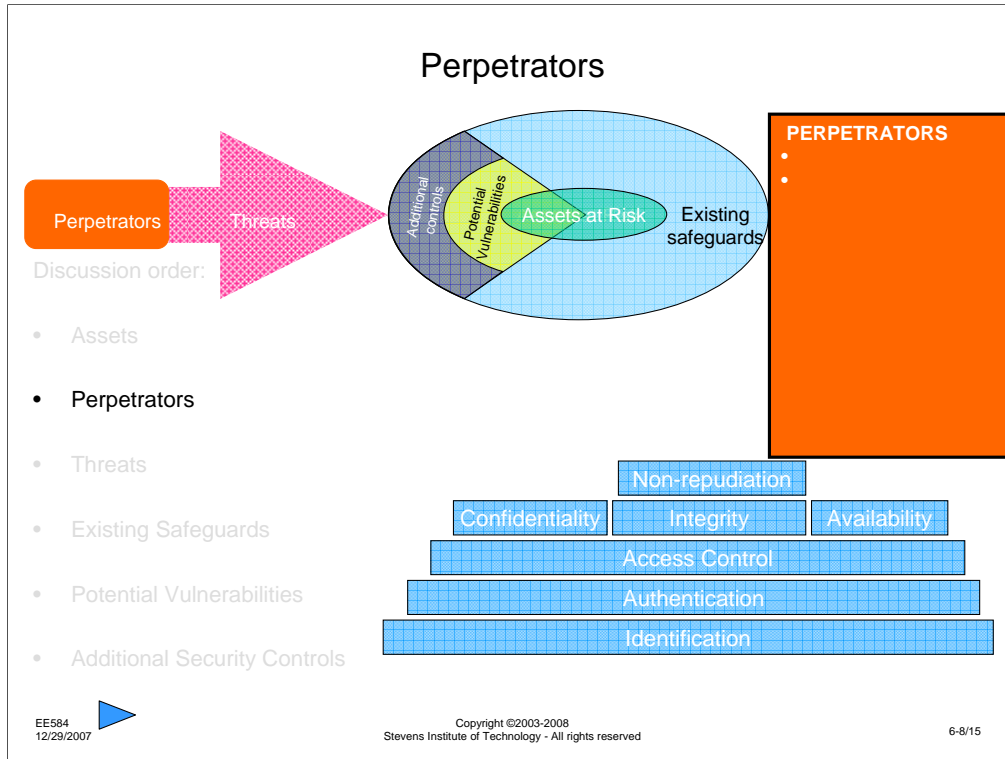
Keep in mind the security architecture at the bottom right. For each security service, there might be something in your system that needs protecting.

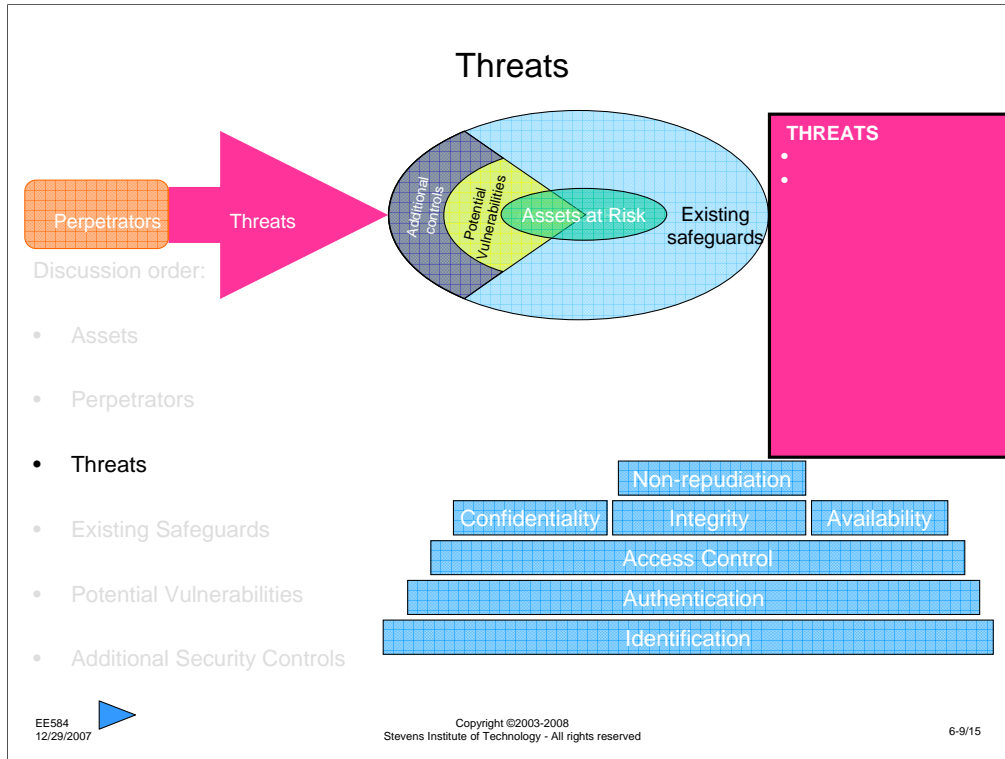


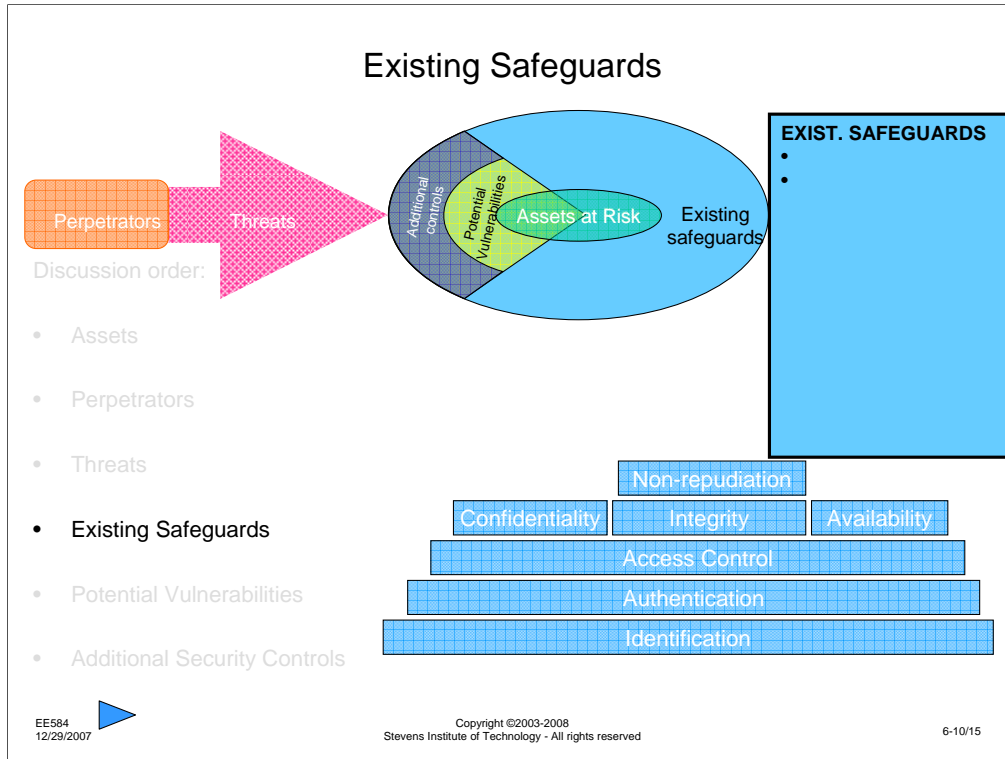
I recommend that as you examine the system under discussion, you create a discussion topic for each aspect of security and/or for each element of the security assessment process. This is a brainstorming process, so don't worry about silly suggestions or things that are not in the right discussion thread. 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.

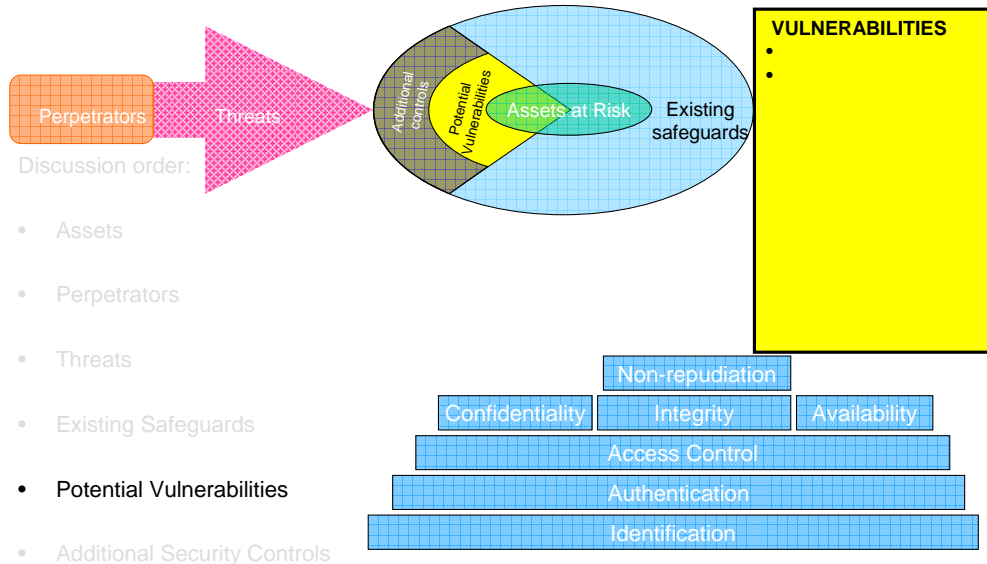
Next week, we will begin another assessment on another system. At that time, I will summarize the discussions and will add some more information about issues in the system that may not have been addressed.







Potential Vulnerabilities



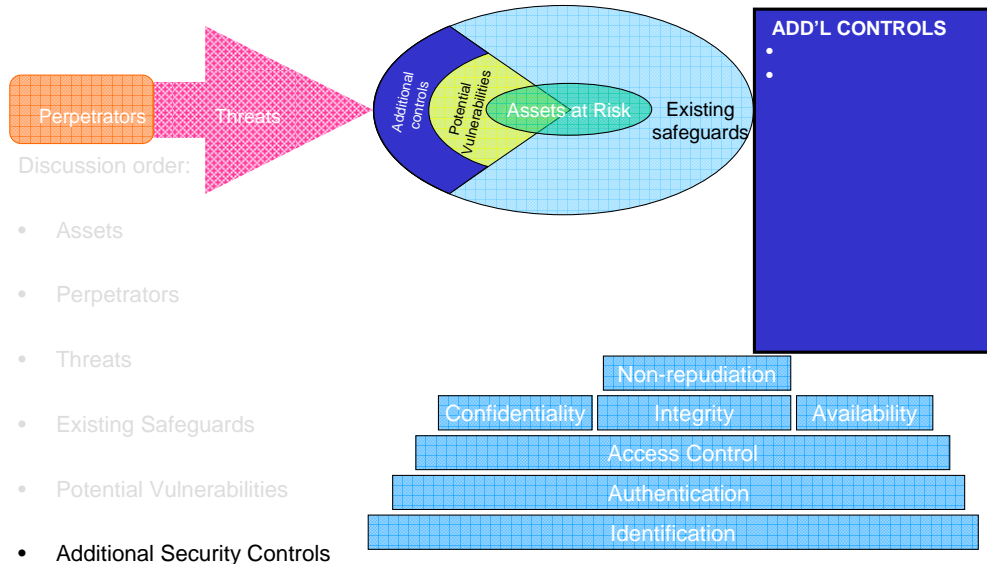
EE584
12/29/2007



Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-11/15

Additional Controls




EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-12/15

ASSETS <ul style="list-style-type: none">••	PERPETRATORS <ul style="list-style-type: none">••	THREATS <ul style="list-style-type: none">••	
	EXIST. SAFEGUARDS <ul style="list-style-type: none">••	VULNERABILITIES <ul style="list-style-type: none">••	ADD'L CONTROLS <ul style="list-style-type: none">••

EE584 12/29/2007 

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-13/15

Case 3 – Military Tactical Radio Systems

30-88 MHz VHF-FM/FSK link
25 kHz channels, 16 kb/s voice/data

FO

Jammer

The diagram illustrates a military tactical radio system. A helicopter is shown at the top, connected by a solid black line to a ground soldier labeled 'FO' (Forward Observer). A dashed black line represents a radio link from the helicopter to a city on the right. A solid black line connects the FO to the city. A pink wavy line represents a jammer's signal, originating from a vehicle labeled 'Jammer' and directed towards the city. A yellow starburst indicates a jamming effect near the city. A green tank is also shown near the city. The background features blue mountains and green hills.

14

Security Technical Paper Assignment

- Follow the instructions from Week 3, Paper 1 assignment, to access the IEEE Conference Proceedings database.
- Pick an article from the Proceedings of IEEE Symposium on Security and Privacy (from the last 5 years) that interests you
- Write a 3-5 page report on the paper. Report should include:
 - Citation of the paper you are using
 - Summary of fundamental ideas presented in the paper
 - Issues paper addresses and how they have been addressed in the past
 - Discussion of 1 or 2 core ideas of paper
 - Identification of any **wireless-related issues** brought up in the paper (there may not be any)
 - Potential applications of technology presented
 - Future opportunities created by the technology

EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

6-15/15

This being Week 6, it is time for the assignment of the second paper. This one is on the general topic of security. As before, the paper is due in two weeks – during Week 8. The overall process is the same, just the potential references are different.

This assignment is to be derived from the IEEE Security and Privacy Proceedings, which is based on the annual conference of an IEEE society. This is NOT the IEEE Security and Privacy magazine, which is published monthly.