Wireless Systems Security

EE/NiS/TM-584-A/WS

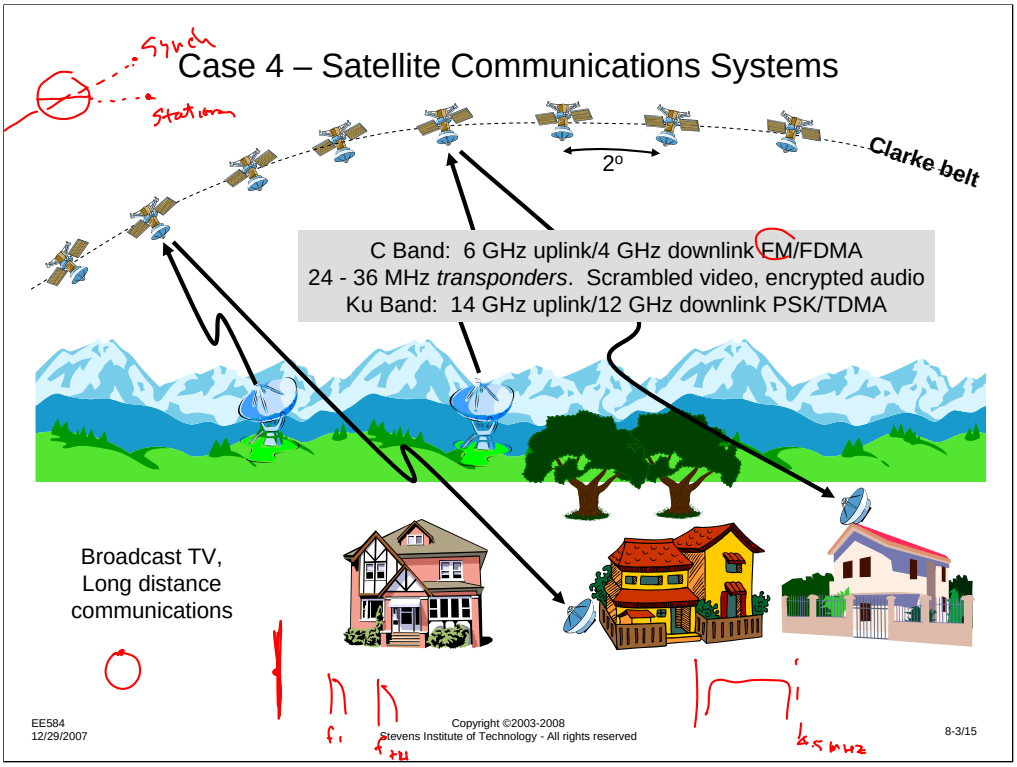
Bruce McNair
bmcnair@stevens.edu

Week 8

Case Study 4

This week we will address the fourth case study. As it was for the last two week, you should discuss the security issues in the WebCT discussion groups I have set up. These are labeled Red Team 4 and Blue Team 4. DO NOT POST THIS WEEK'S DISCUSSION TO THE TEAM 2 OR 3 GROUPS. It may not be read by other students and will certainly be confusing. Don't post items that should be in your group's discussion to other discussion groups, such as Main, either, since (a) we are trying to keep the Red and Blue team perspective different and (b) other students may not go looking for the assessment discussions there.

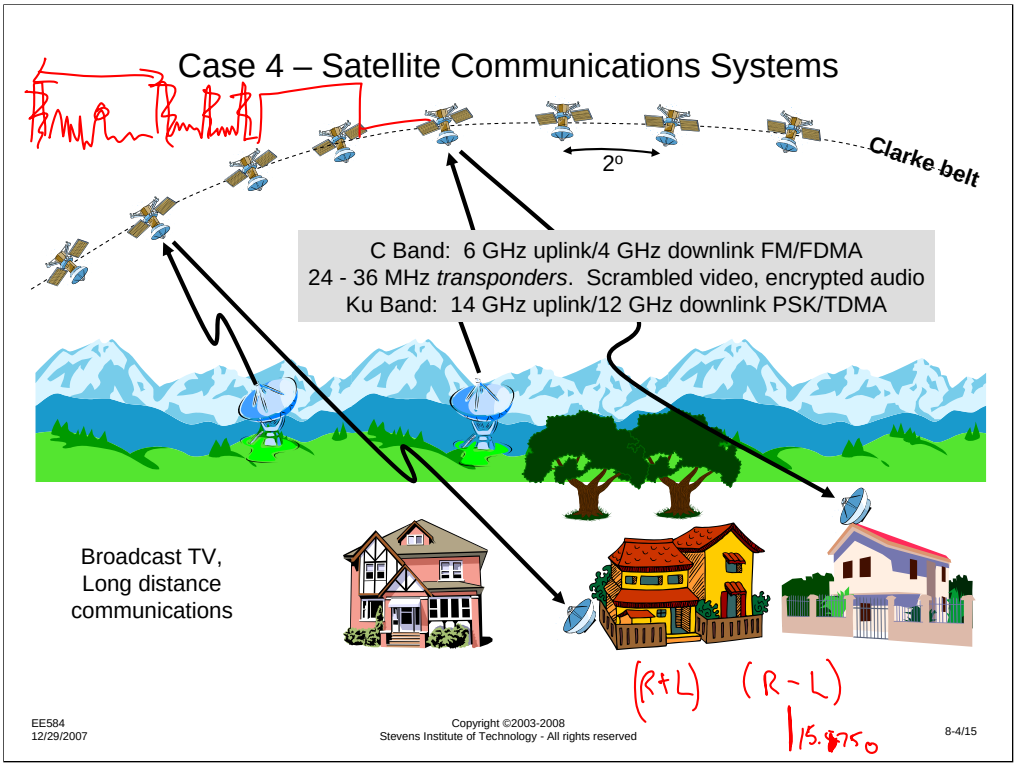
This week, I randomized the teams as I did for the first assessment. I will continue to do this for the rest of the assessments.



This week's assessment deals with satellite communications system. You may currently think of satellite communications systems in terms of the 14/12 GHz Ku-band DISH network and other so-called small (18-24 inch) dish systems, but this is only part of the environment. Prior to the digital systems that are in use at Ku band, there were, and still are, many C -and systems that operate at 6 GHz/4 GHz, and depend on 10-16 foot dishes. These are the analog systems that originally started satellite TV and have been used extensively for remote news feeds, network distribution, and home satellite TV systems. While the all digital Ku-band systems have the option of encrypting all of the programming, both video and audio, the older C-band systems generally used scrambled analog video and only encrypted the audio portion of the broadcast. For most TV programming, the entertainment value is greatly degraded when the audio is eliminated. Of course, there is some programming for which the audio is irrelevant, but the entertainment industry is mainly interested in restricting access to content with the broadest interest.

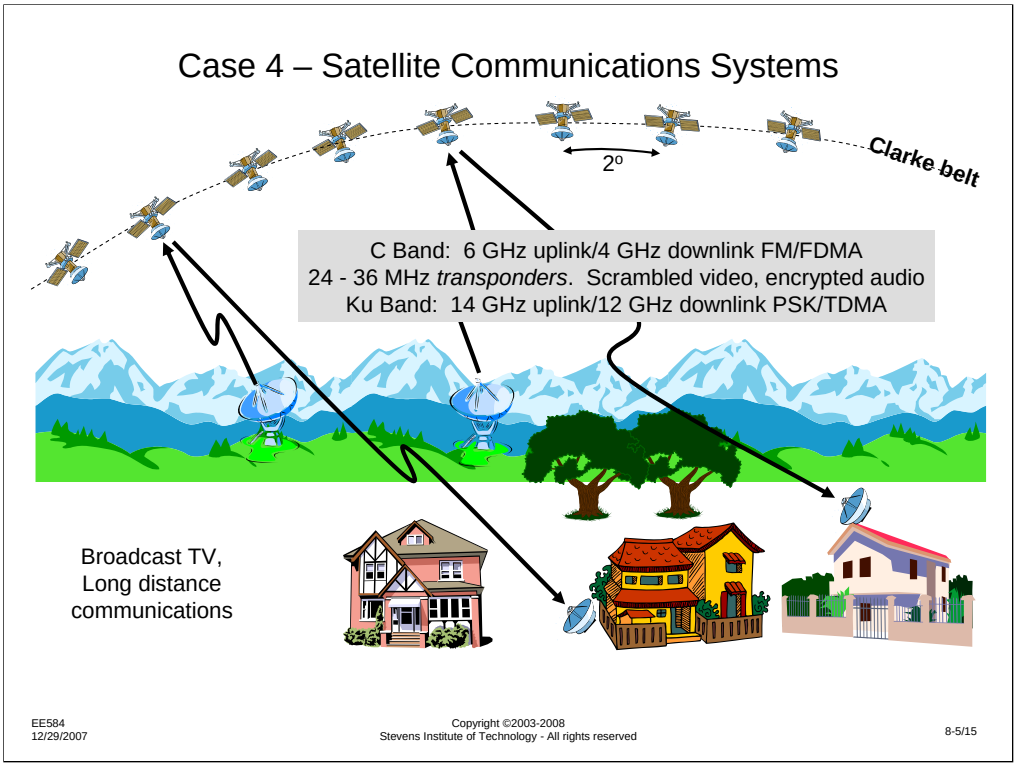
In addition to the TV programming, the analog C-band systems have also been used for distribution of high quality audio programming (e.g., FM radio networks), and multichannel long distance telephone traffic. Of course, the widespread availability of long haul fiber networks has reduced the need for satellite long distance networks, but there still is a fair amount of voice traffic carried on satellite systems, particularly to remote areas where it would not be economical to string fiber. We will concentrate out discussion of satellite communications system security on the analog C-band systems to illustrate some of the generic issues with wireless systems security.

In order to simplify the satellite tracking problem that Earth stations would otherwise face, communications satellites are generally placed in orbit in the so-called Clarke belt. This is a region 24000 miles from the Earth above the Equator. Satellites in these orbital positions appear to be fixed in space, since they rotate at the same speed as the Earth and do not drift North or South. This is called the Clarke Belt in honor of Arthur C. Clarke who first described the concept of a geosynchronous satellite in 1940s science fiction.



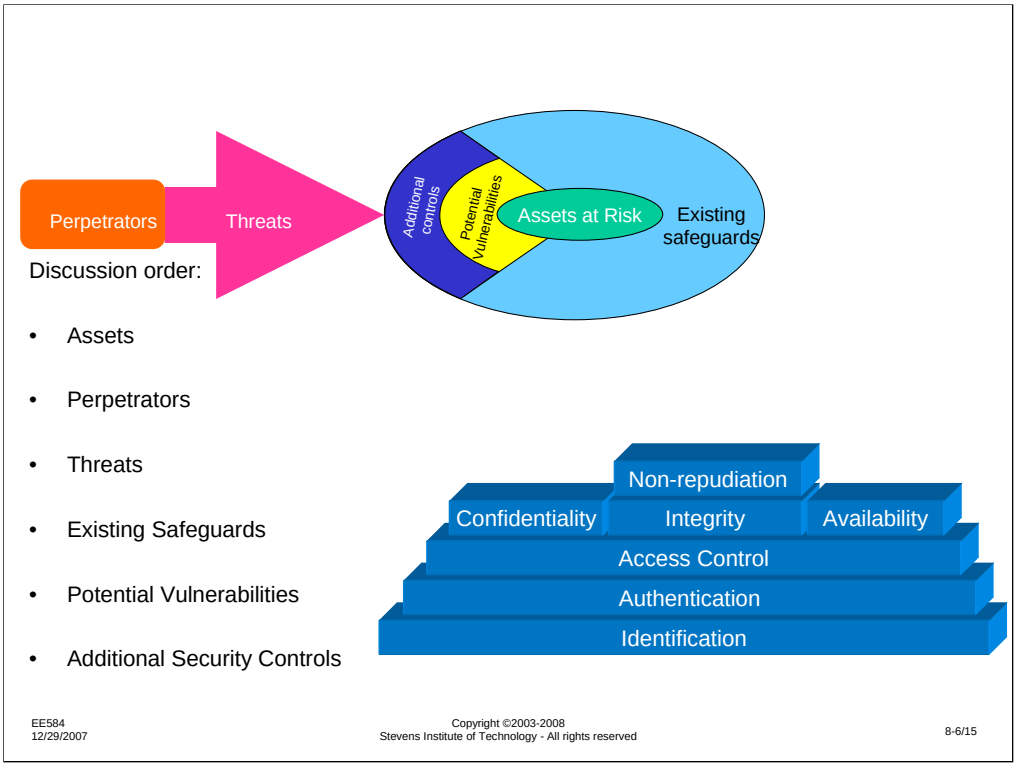
There are a few parameters of the geosynchronous satellite communication system dictated by the orbital position. First, the sheer distance to the satellite creates a very high path loss. This means that signal levels at the satellite receiver and the ground station receiver are very low. Because the satellite must operate without an energy source other than solar cells, batteries must store energy for when the satellite is in the Earth's shadow. This limits the amount of power the satellite transmitter can generate. High gain antennas on the ground are needed to be able to receive the low level signals. The uplink power is not so constrained, since the Earth station transmitter can run from the AC power mains. Despite the large Earth station antennas and their relatively narrow beamwidth, there are still a relatively small number of orbital positions – each satellite needs to be about 2 degrees apart in orbit. Further, satellite orbits tend to drift due to gravitational and other forces. This means that some mechanism is needed for "station keeping" – ongoing corrections to keep the satellite in its proper position. Generally, the limitation in the amount of fuel that can be used for long term station keeping is the item that sets the useful lifetime of the satellite. Once the station keeping fuel is nearly exhausted, the remaining fuel must be used to move the satellite out of its orbital position (generally by moving it further from or closer to the Earth) to allow a new satellite to be put in its place.

One important element of the overall satellite communications system is the control link. It is this channel that is used to send station keeping commands to the satellite and to receive telemetry about the health of the satellite, its batteries, and its fuel level. Generally, the same ground station that transmits information for relaying by the satellite is used for managing the satellite operations.



Much like the channels of a terrestrial TV receiver, a home satellite receiver is capable of tuning to different frequencies transmitted by a single satellite. These “channels” are referred to as “transponders.” The reason for this is that most satellites operate as simple relay sites. Signals that are transmitted up to the satellite on a particular band of frequencies at the C-band satellite 6 GHz uplink are translated by a fixed amount to a corresponding set of frequencies at the 4 GHz downlink and are retransmitted. One 36 MHz wide band of frequencies is referred to as one “transponder.” In all, C-band satellites are configured to have 24 separate transponders, so each satellite can relay 24 distinct channels. (Note 1: the oldest C-band satellites had 12 transponders. Note 2: While one TV video signal, along with a few associated TV audio and miscellaneous FM radio quality audio channels occupies one transponder, one transponder can carry hundreds of analog phone channels.) To maintain the highest video signal quality, so-called “studio quality,” signals, a TV signal that would occupy 6 MHZ for terrestrial transmission occupies a 36 MHz transponder, since the signal is frequency modulated with a relatively high modulation index. The use of FM also provides a signal that is insensitive to amplitude variations and can be transmitted through a high-efficiency nonlinear amplifier on the satellite.

The final item of note for a satellite communications system is the so-called “footprint.” While some of the more modern satellites are capable of directing their downlink to selected areas, most satellites transmit signals that have coverage areas the size of the entire continental US and significant portions of the rest of North America. Anyone in the “footprint” of the satellite is capable of receiving the satellites signal.



As for the previous assessments, 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?

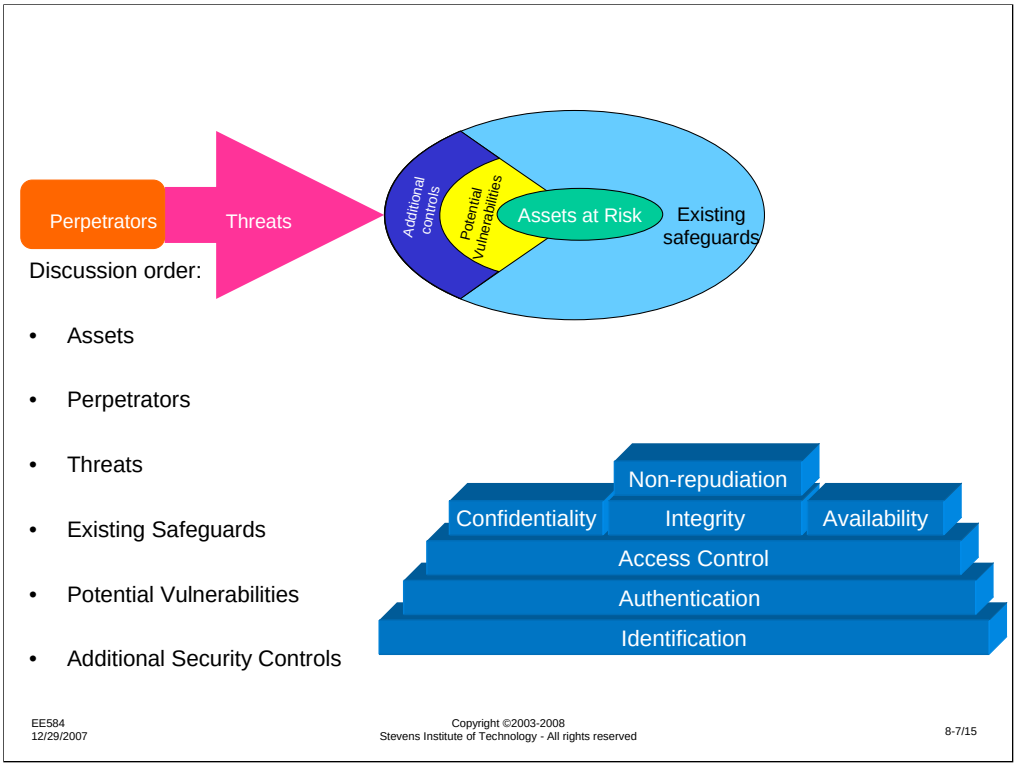
Threats: What mischief can you get into? How would you do it?

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.



Again, 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?

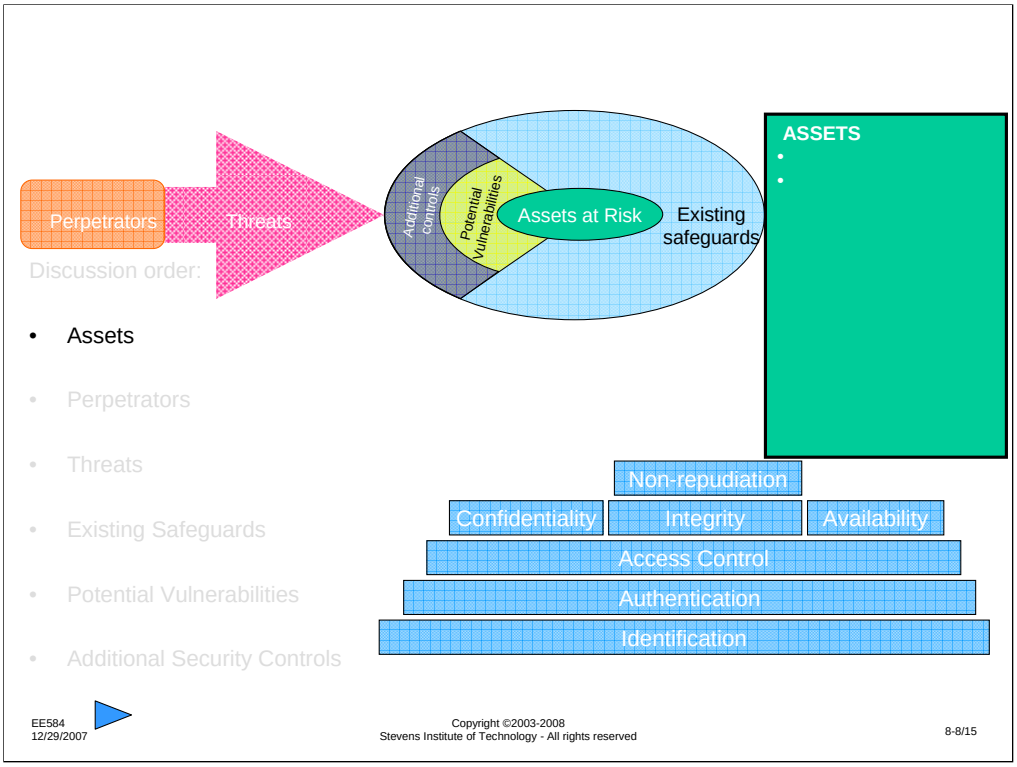
Threats: How might someone try to attack your system?

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?

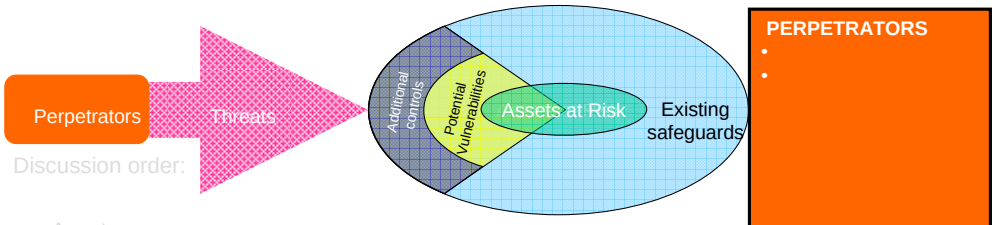
Keep in mind the security architecture at the bottom right. For each security service, there might be something in your system that needs protecting.



Once 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.

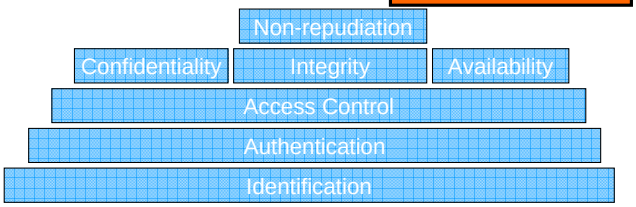
Again, the Red Team will not be able to see the postings of the Blue Team during this week and vice versa. As I did previously, next week, both sets of discussions will be open to the other group. I encourage each group to compare their thought process with the process of the other group. You can, however, 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.

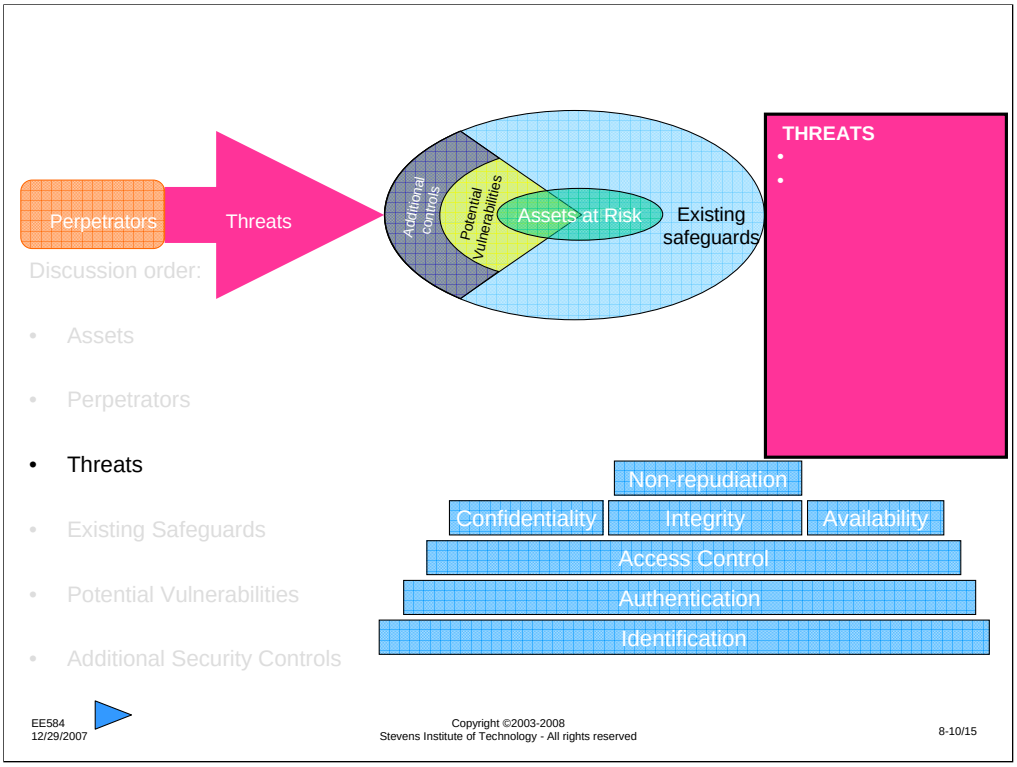
Next week, we will begin another assessment on another system. At that time, again, I will summarize the discussions and will add some more information about issues in the system that may not have been addressed.

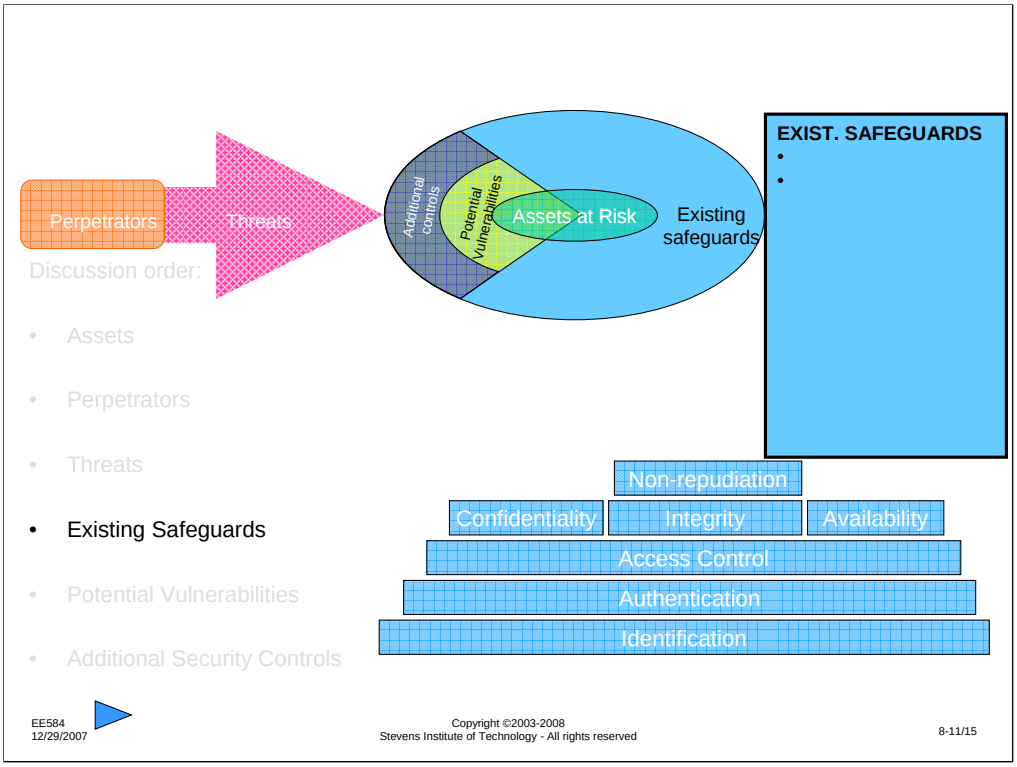


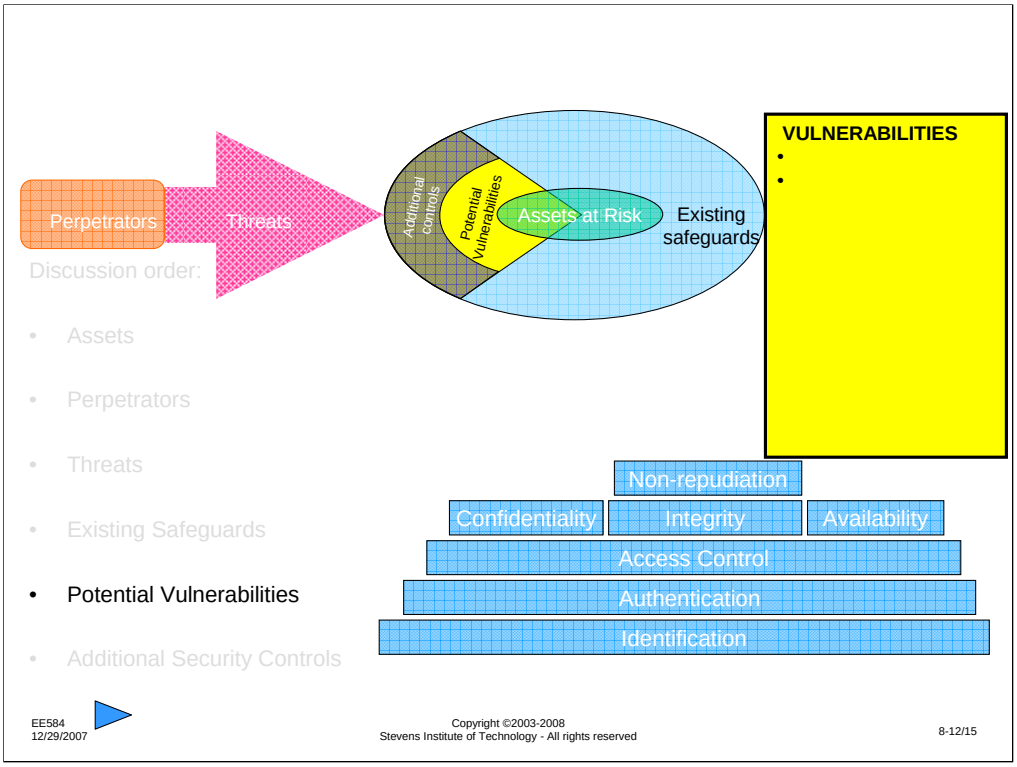
Discussion order:

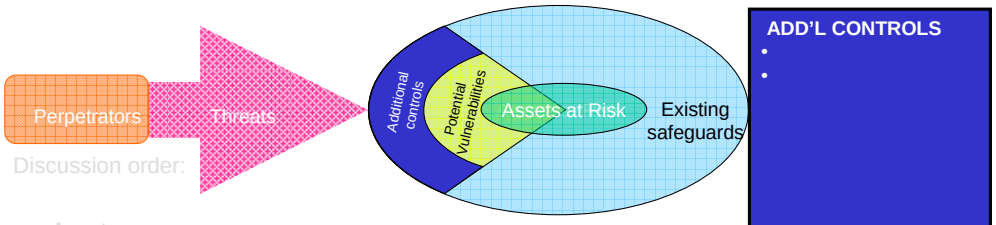
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls




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
12/29/2007
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
8-10/15


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
12/29/2007
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
8-11/15


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
12/29/2007
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
8-12/15

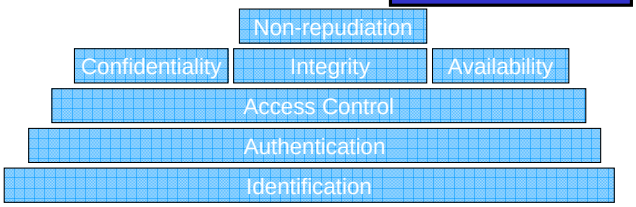


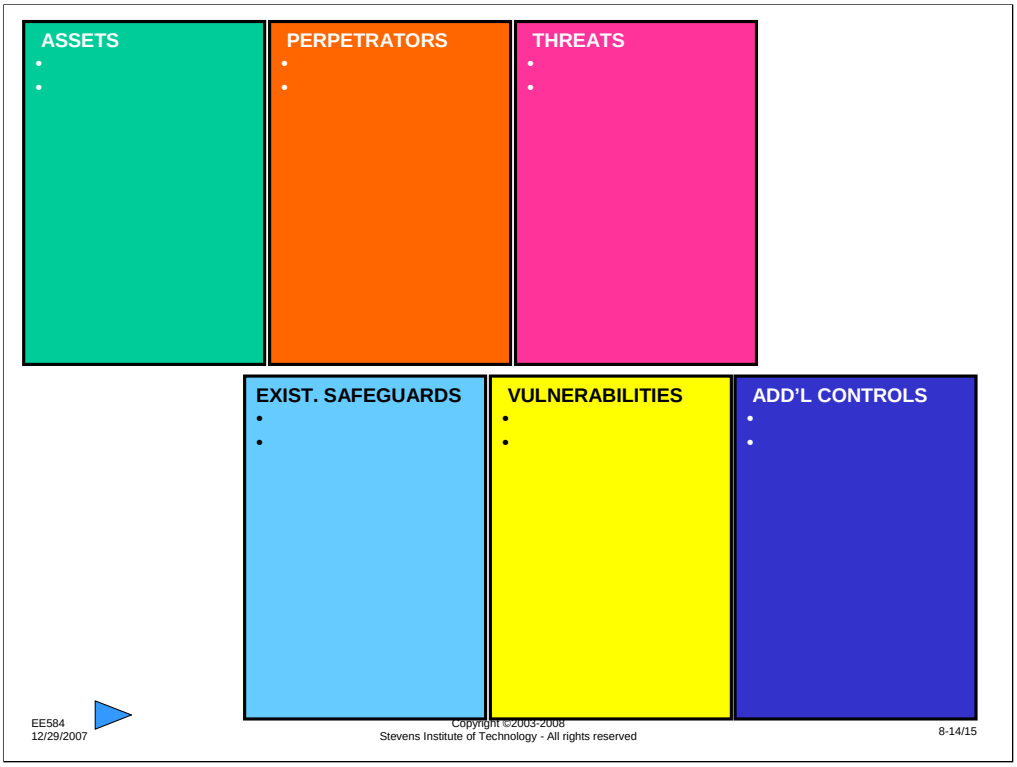
ADD'L CONTROLS

-
-

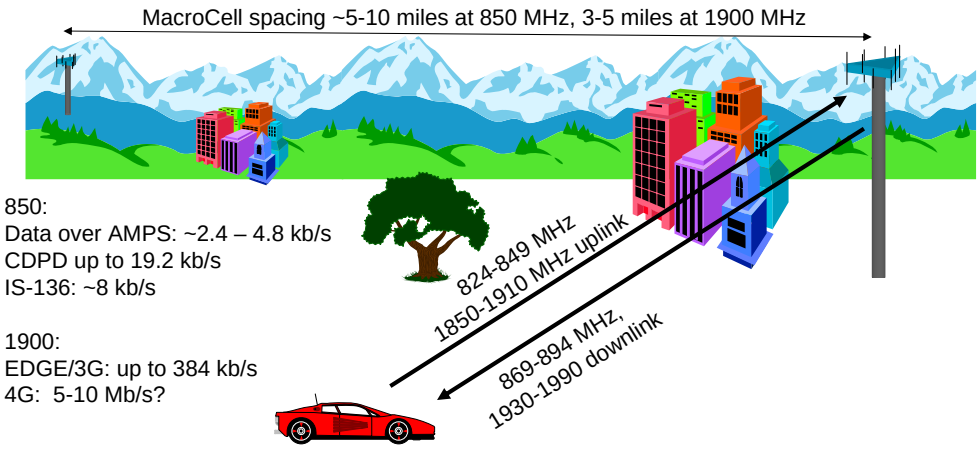
Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls




ASSETS
PERPETRATORS
THREATS
EXIST. SAFEGUARDS
VULNERABILITIES
ADD'L CONTROLS
EE584
12/29/2007
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved
8-14/15

Case 5 – Wide Area Wireless Data Services
CDPD, 3G, EDGE, etc.



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?

Next week, we will be assessing wireless wide-area data services. Some of the systems that exemplify these types of services are CDPD, 3G, GPRS, EDGE, 1xRTT, and EVDO. Research some of these systems to understand the applications and how the security issues they may exhibit.