

# 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

11-1/15

# Week 11

## Case Study 7

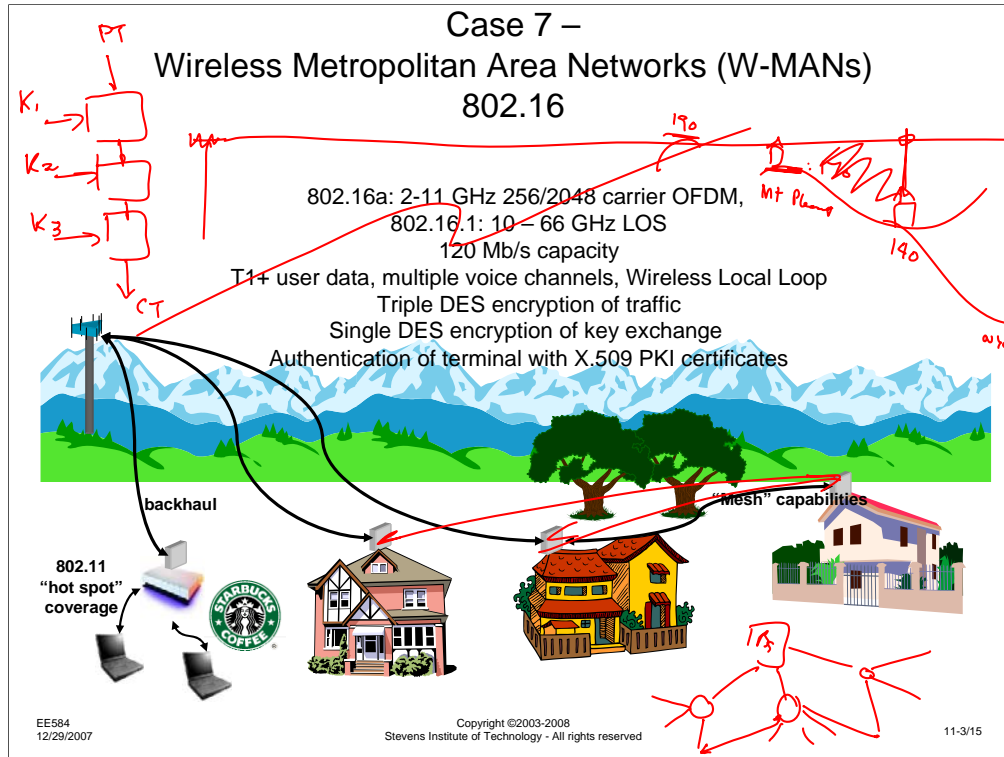
EE584  
12/29/2007

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

11-2/15

This week we will address the last case study for the class. As it was for the previous weeks, you should discuss the security issues in the WebCT discussion groups I have set up. These are labeled Red Team 7 and Blue Team 7. **DO NOT POST THIS WEEK'S DISCUSSION TO THE TEAM 2, 3, 4, 5 or 6 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 again randomized the teams as I did for the first assessment. I will continue to do this for the rest of the assessments.



The wireless network for this last case study is a newly emerging set of standards addressing what are known as wireless MANs – Metropolitan Area Networks. As the name implies, this is a broader coverage area than a WLAN, capable of covering a metropolitan area, perhaps several square miles to dozens of square miles. You might consider the coverage area to be similar to the coverage of a cell site.

One notable difference between WMANs and cellular networks is the fixed locations of the WMAN base stations and subscriber terminals. This means that the network planner does not need to deal with the second by second variation in the channel quality. In general, a subscriber terminal location is chosen, the antenna is directed at the base station, and the network remains static for long periods of time. Seasonal changes in foliage or building construction are likely to be the most rapidly changing aspects of the gross system environment, making it much easier to design a high speed system.

Three distinctly different forms of using a WMAN are shown above:

- (1) The easiest to understand is shown to the left of center – a residence is directly in touch with the base station.
- (2) On the far right side of the chart, a subscriber location is not able to access a base station directly, perhaps because of an obstruction blocking the path. To the left of this subscriber is another customer who is able to access the base station. By using a so-called mesh network, the blocked subscriber relays their signals through an intermediate subscriber location, enabling the communications path.
- (3) There has been a growth of 802.11b "hot spot" coverage. Starbucks was one of the first to provide 802.11b Internet access in their coffee shops, presumably to entice customers to spend more time at the coffee shop and purchase more coffee. McDonalds has discussed doing the same (giving a whole new meaning to the protocol MAC layer). Airports and other places where people are likely to congregate for long periods of time are other sites that have been discussed for hot spot coverage. But for any of these networks, how does one provide "backhaul" – to get the bulk data back to the wired network?

## Case 7 – Wireless Metropolitan Area Networks (W-MANs) 802.16



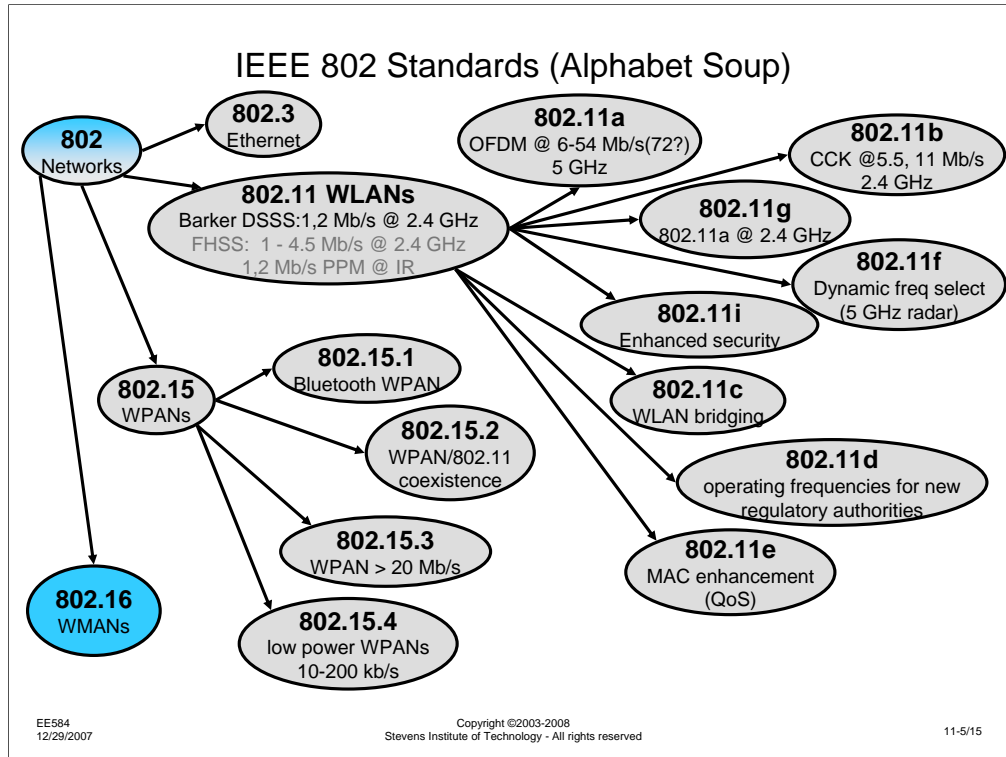
Like 802.11a, the 802.16a standard defines OFDM as the modulation technique to convey high data rates over the fading channel in the region from 2 – 11 GHz. 802.16.1 has received several contributions with different modulation techniques for line of sight systems operating between 10 and 66 GHz.

Generally the 802.16 systems are targeting aggregate data rates on the order of 120 Mb/s. These channels would be able to support end user data rates at cable modem-like speeds (T1 is 1.544 Mb/s). Alternatively, the channel could be used to support multiple voice channels, providing a Wireless Local Loop. Obviously, this would be a desirable capability for companies that want to break the access channel advantage that the RBOCs/LECs (Regional Bell Operating Companies/Local Exchange Carriers).

Acknowledging the encryption issues that were created in 802.11, 802.16 has standardized on Triple DES for the traffic and single DES for the key exchange.

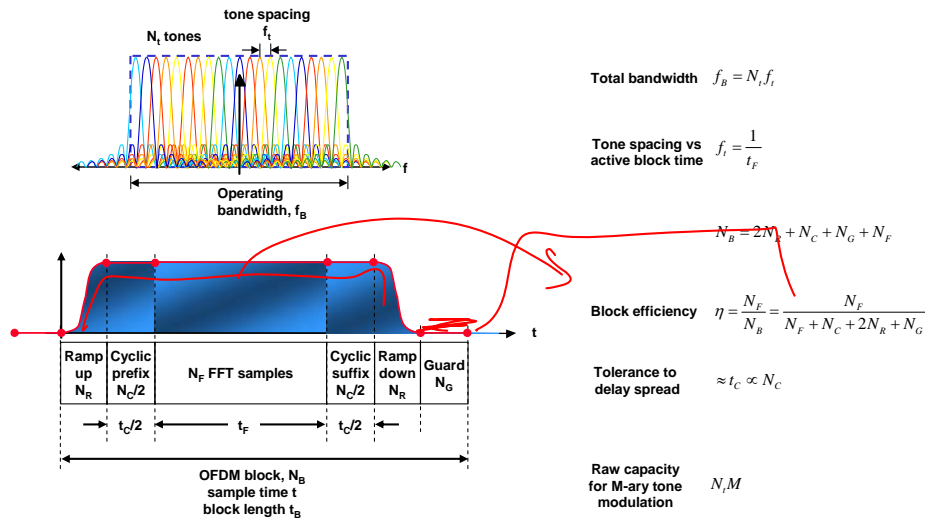
(Triple DES passes a plaintext block through the DES algorithm 3 times, each time with a different 56 bit key variable. This might seem to create an encryption algorithm with a 168 bit key variable, but because of so-called meet-in-the-middle attacks, the effective key variable size is only twice the original size – 112 bits)

Finally, 802.16 has defined a mechanism for the base station to be able to authenticate the subscriber equipment. The X.509 standard defines a Public Key Infrastructure where authentication certificates are exchanged, providing proof to the base station that subscriber unit is not a rogue unit.



We saw this chart last week, but I added it here to remind you how 802.16 fits into the IEEE 802 Networking standards. Where feasible, common signaling formats and messages are used to define new standards, building on the older ones that have been proven in the field.

## OFDM Basics



EE584  
12/29/2007

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

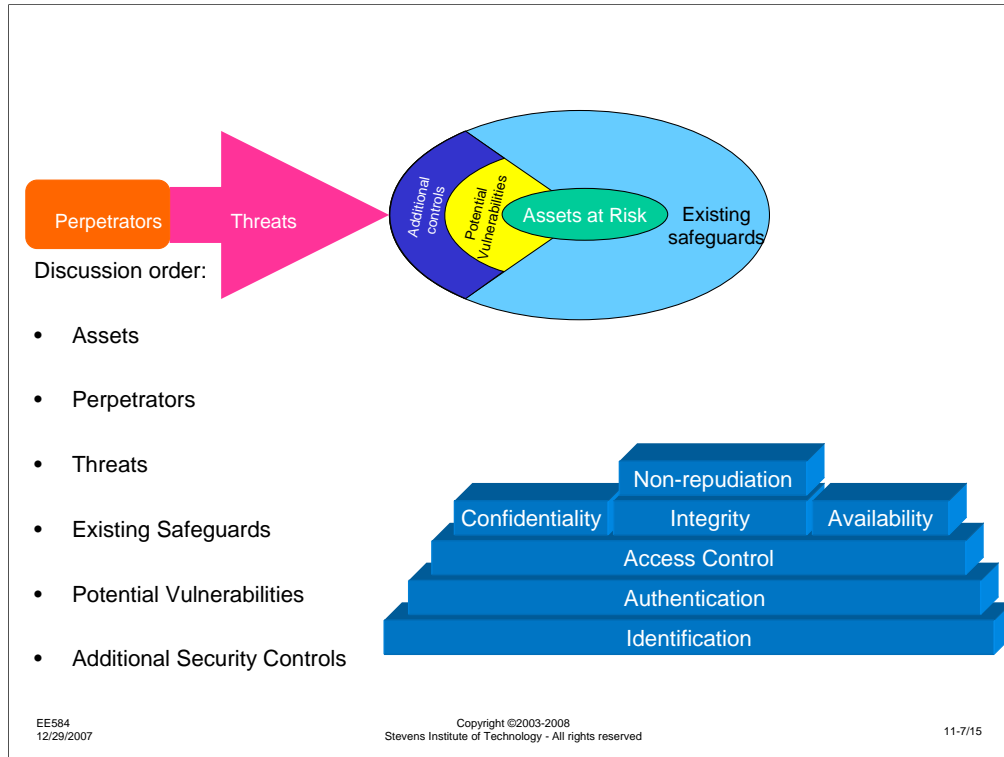
11-6/15

Here, again, is a slide I used for the 802.11a WLAN. For the exact same reasons that OFDM made sense for an indoor WLAN, it also makes sense for an outdoor WMAN. The main difference is the values chosen for various parameters.

802.11a extends the active region of FFT samples by a 800 ns guard interval, allowing tolerance of about 400 ns of delay spread. In outdoor environment, it is not unusual to see a few microseconds of delay spread, requiring a guard interval of, perhaps, 10 microseconds. Just extending the guard interval would significantly degrade link efficiency – 802.11a has a block length of 4 microseconds, so it is inconceivable to use almost all of the block for guard interval. Thus, outdoor OFDM systems must increase their block length to maintain a reasonable efficiency. So, it is not unreasonable to assume a 10 microsecond guard interval in a 50 microsecond block. But the block length determines the OFDM carrier spacing. While 802.11a uses a 312.5 kHz tone spacing (the reciprocal of the 3.2 microsecond active region), an outdoor OFDM system with a 40 microsecond active region would have a 25 kHz tone spacing.

Since OFDM can only convey symbols at the block rate, this means that a system with a 50 microsecond block length (40 microsecond active region plus 10 microsecond guard interval) has a symbol rate of 20 kbaud. To achieve data rates of 10s to 100 Mb/s, this means that the number of OFDM carriers must be far more than the 52 carriers used in 802.11a. If we were to design a system with 2048 carriers, each carrying 2-4 bits per symbol, data rates of 80 – 160 Mb/s could be achieved, allowing overhead for channel error coding, synchronization, and signaling. The 2048 carriers, with a 25 kHz spacing, would require an RF bandwidth of 50 MHz.

The argument for OFDM in 802.11a were part of what delayed the standard until after 802.11b came out. No one was really sure if it would work. In contrast, there was little argument about the suitability of OFDM for 802.16 – the European DVB-T (Digital Video Broadcasting – Terrestrial) standards, the DAB (Digital Audio Broadcasting) standards, DSL, cable modems, etc., have all proven the effectiveness of this modulation method.



Once again, 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?

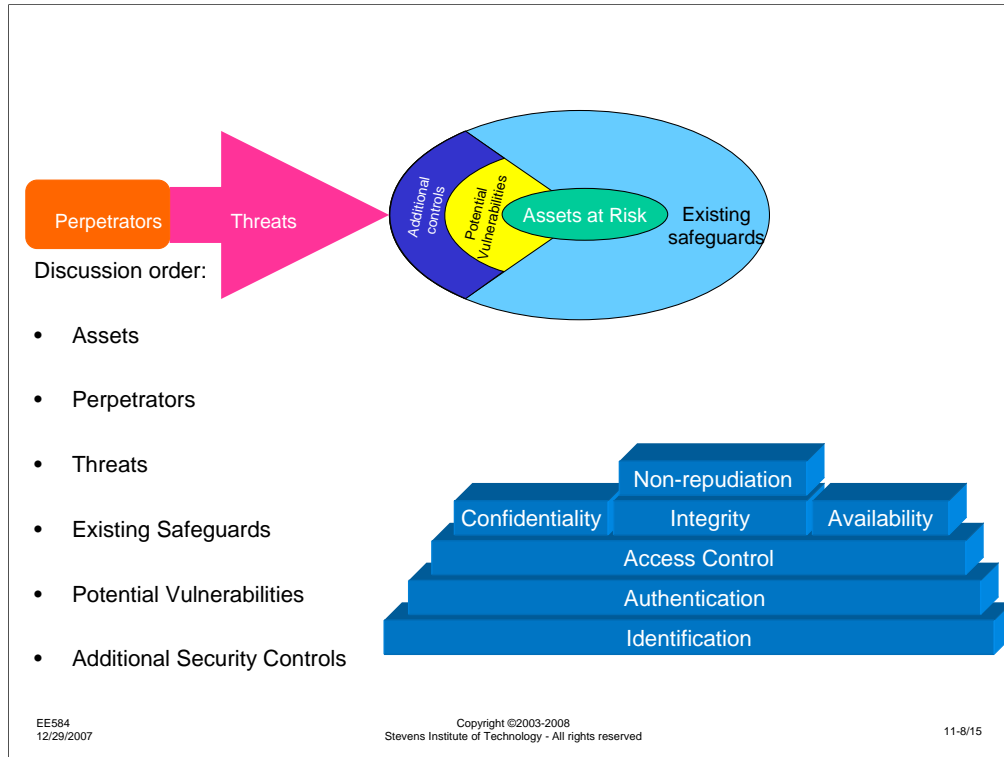
**Threats:** What mischief can you get into? How would you do it?

**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?

Again, 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?

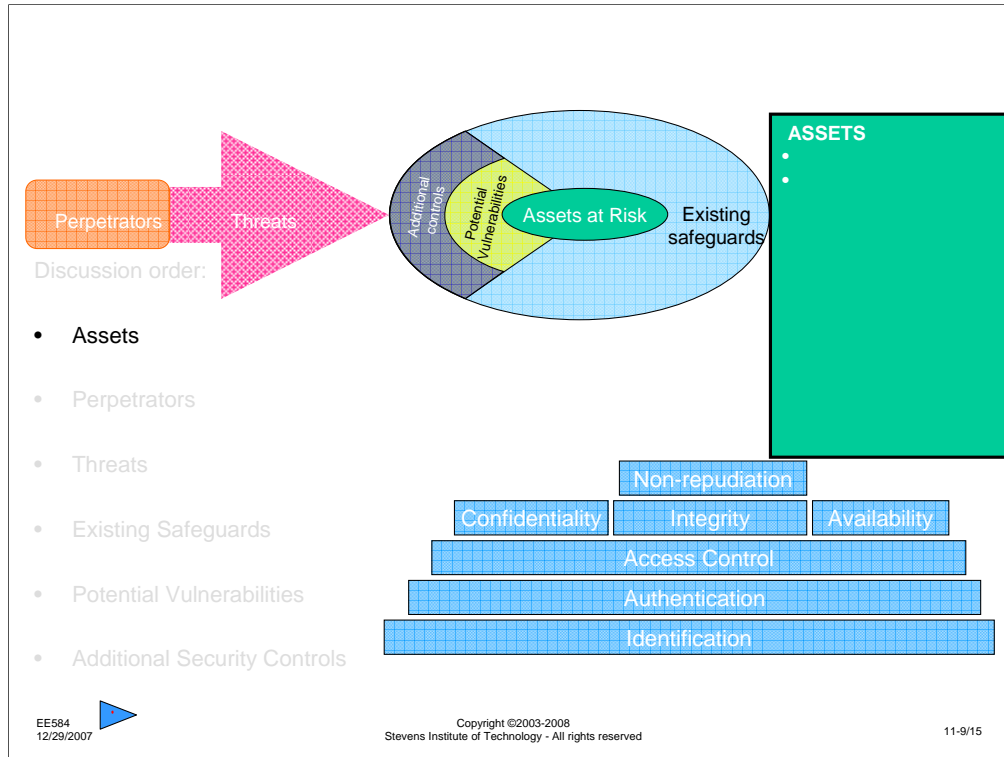
Safeguards: What protection is already in place?

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?

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



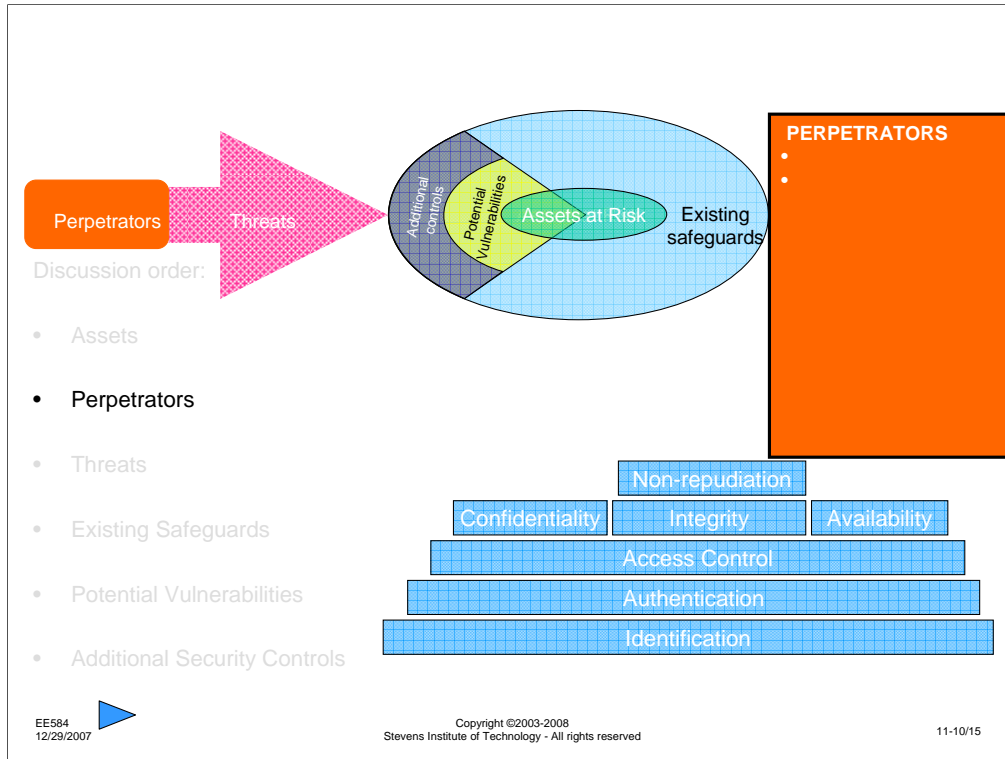


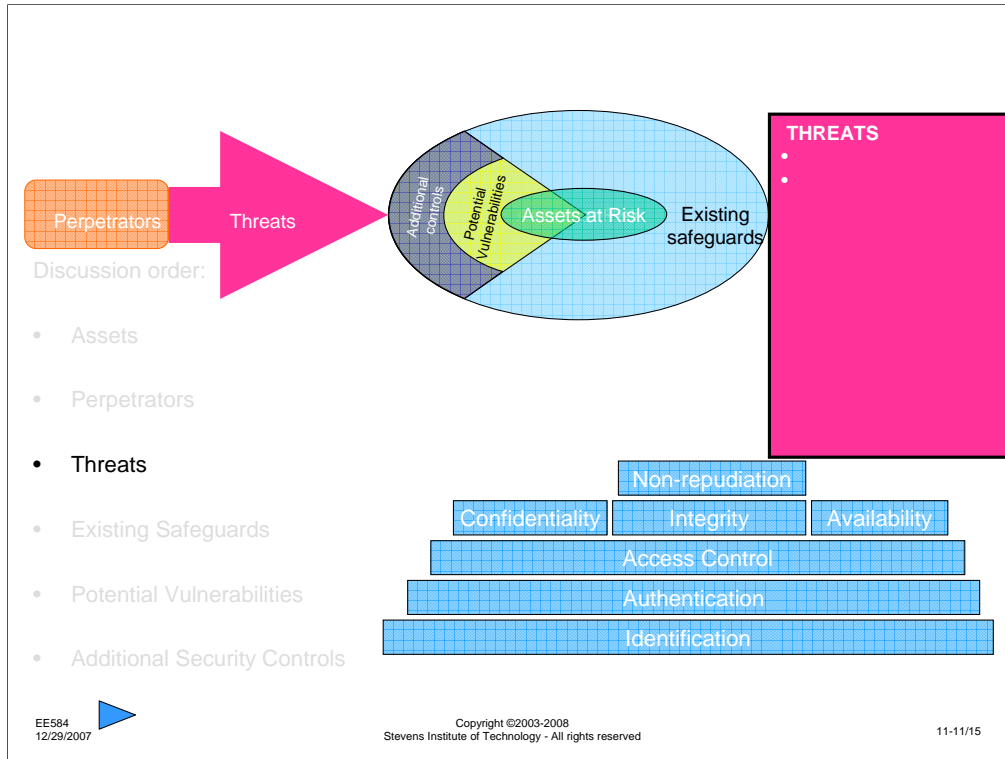
Once again, I recommend that as you examine the system under discussion, you create a discussion topic for each aspect of security and/or for each element of the security assessment process. This is a brainstorming process, so don't worry about silly suggestions or things that are not in the right discussion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

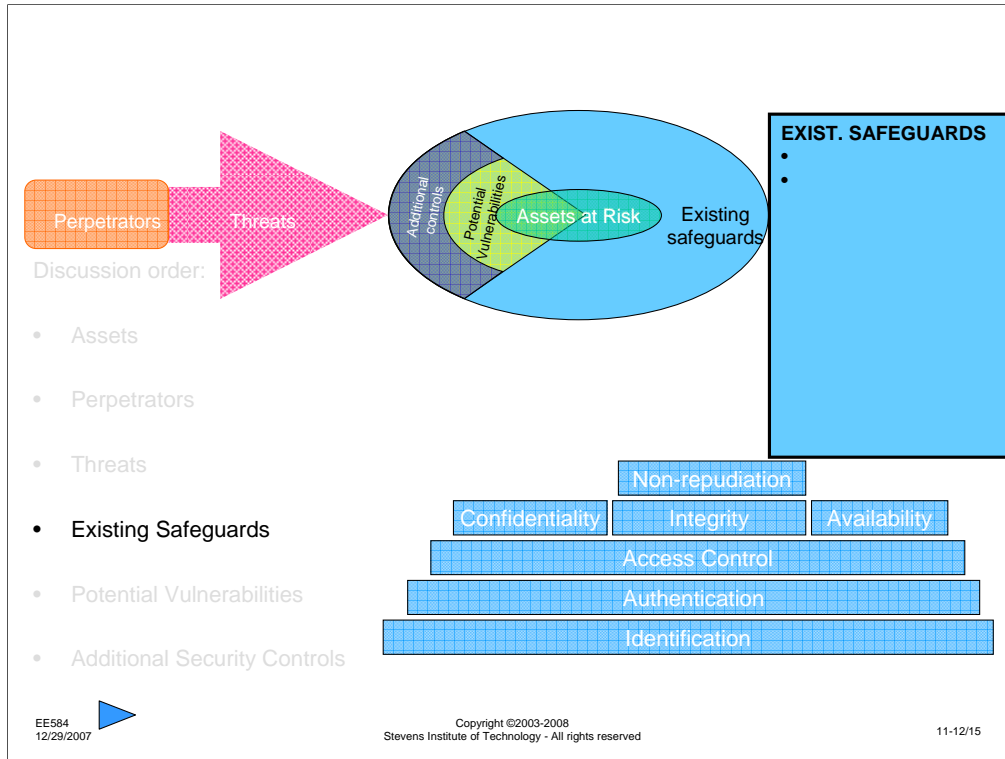
Again, the Red Team will not be able to see the postings of the Blue Team during this week and vice versa. As I did previously, next week, both sets of discussions will be open to the other group. I encourage each group to compare their thought process with the process of the other group. You can, however,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

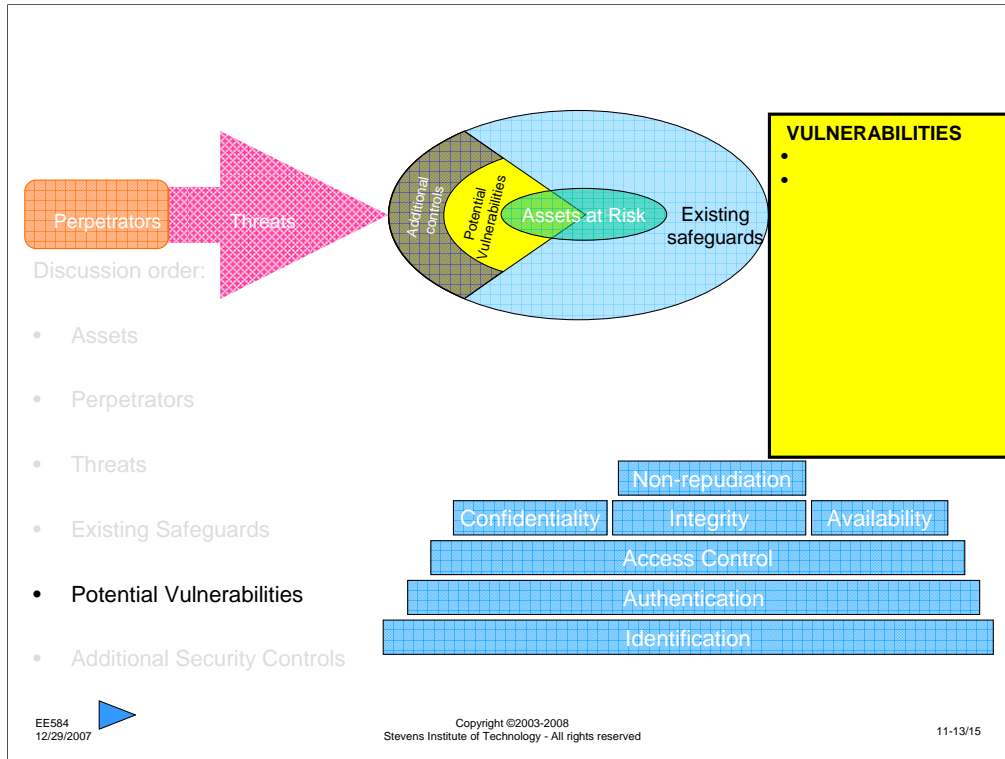
This is the last assessment. After the week is over, I will again post a wrapup of this assessment.

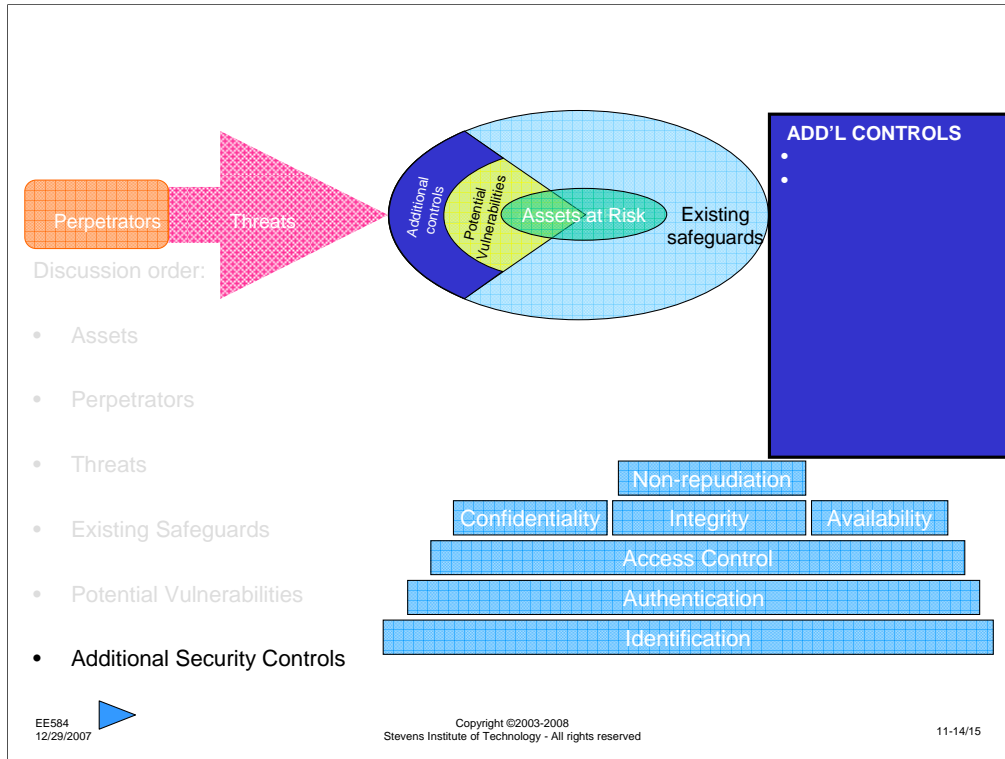
The slides for next week will summarize several of the lessons I hope you gathered from these discussions.












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

EE584 12/29/2007 

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

11-15/15