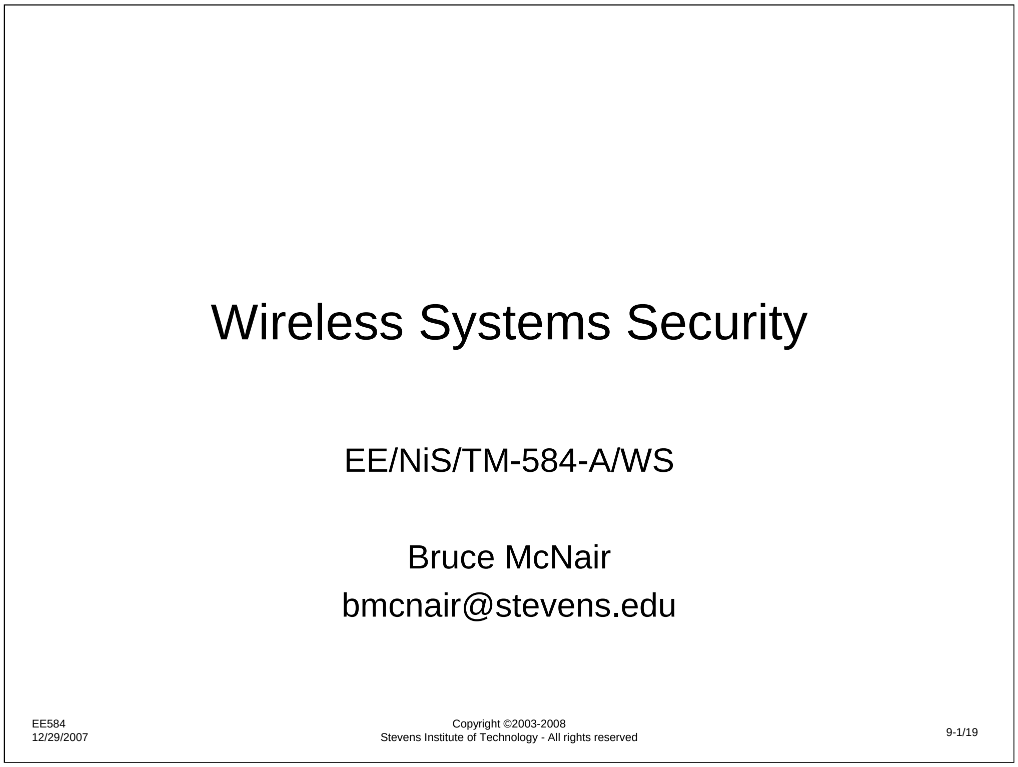
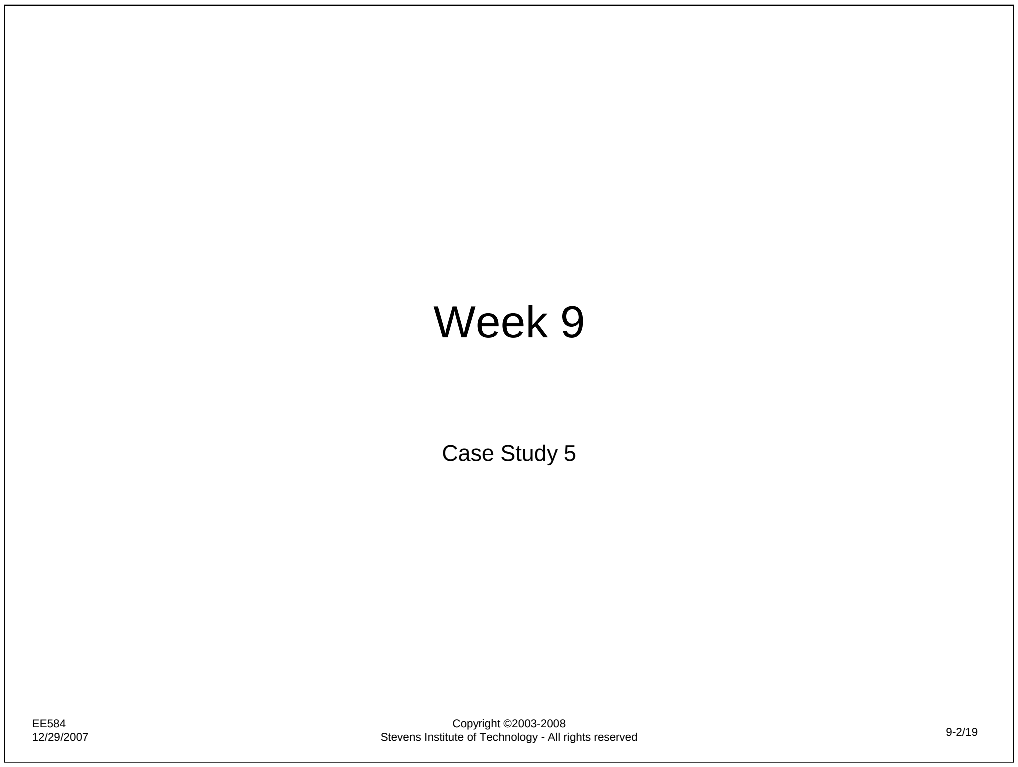


Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

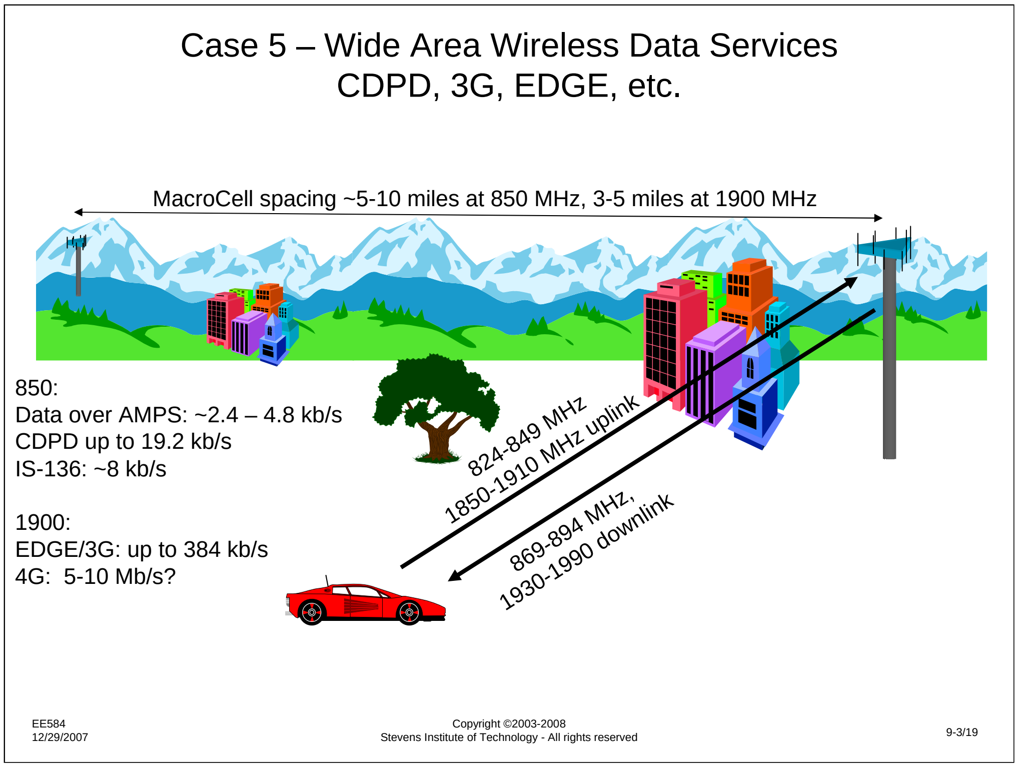


Week 9

Case Study 5

This week we will address the fifth case study. 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 5 and Blue Team 5. DO NOT POST THIS WEEK'S DISCUSSION TO THE TEAM 2, 3, or 4 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.



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

MacroCell spacing ~5-10 miles at 850 MHz, 3-5 miles at 1900 MHz

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?

824-849 MHz
1850-1910 MHz uplink

869-894 MHz,
1930-1990 downlink

EE584
12/29/2007

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

9-3/19

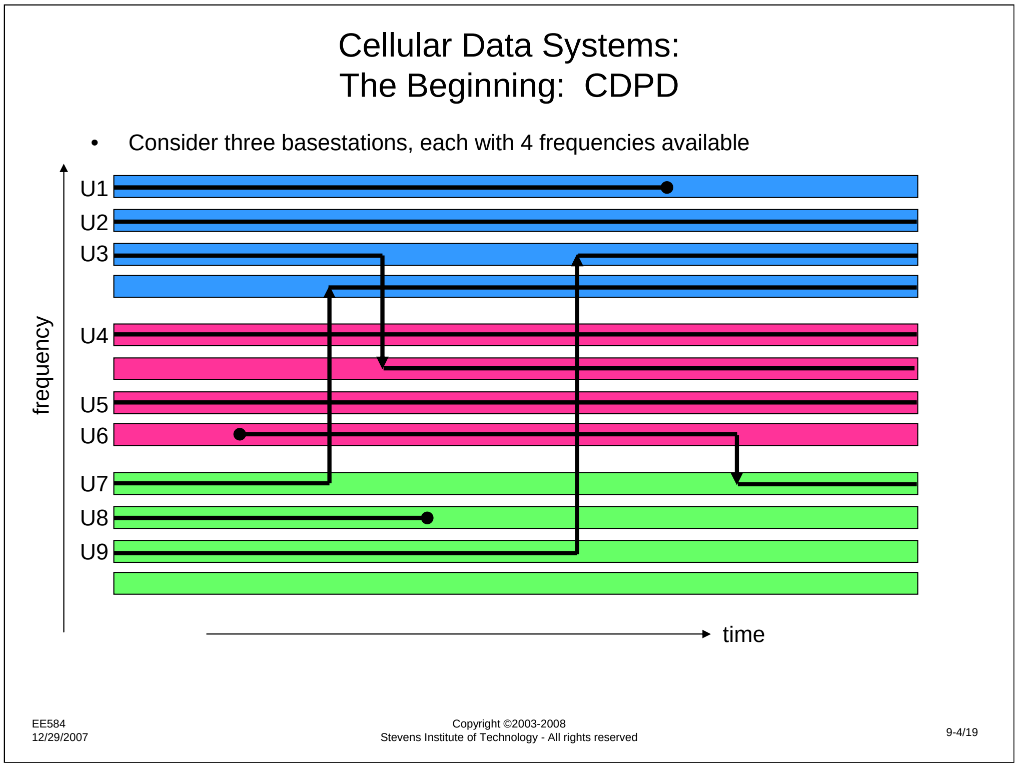
For this week’s assessment, we will be dealing with the emerging set of services known as wide area wireless data services.

Shortly after analog AMPS was fielded, it was recognized that data services would be a useful addition to wireless voice services. The first attempts at wireless data services attempted to use dial-up analog modems with analog AMPS handsets. While the landline analog channel is capable of supporting data rates up to 53 kb/s, it is not feasible to attain these data rates over an AMPS channel. First, the fading on the channel tends to create higher error rates. Voice signals are immune to short drop-outs, sometimes unnoticable to the user. However, with symbol periods on the order of milliseconds, interruptions that would not bother speech wipe out several bits, making the data unusable. Nevertheless, there were attempts to send analog signals over the channels at low data rates. The next problem that the user encounters is the loss of data carrier when a handoff occurs. This would normally lead to a dropped dat call, but modems that were settable to longer carrier dropouts were able to handle this.

The second generation IS-136 system is inherently a digital transmission system, so it would seem that it should be possible to send data via this system. Unfortunately, the digital path was designed for voice signals, and is not optimized for data transmission. Again, systems have been deployed that provide up to 8 kb/s data rates.

The first practical wide area wireless data service was CDPD – cellular digital packet data, a system that is still available today, although not as it was originally designed. This system will be described in more detail in the next slides.

With the evolution to 3rd generation cellular systems, data services have received greater emphasis, as evidenced by EDGE and other 3G systems that promise shared data rates up to 384 kb/s. 4th generation systems are in the planning stages and may offer data services up to 5-10 Mb/s. The rationale for these systems will also be discussed in the next few slides.



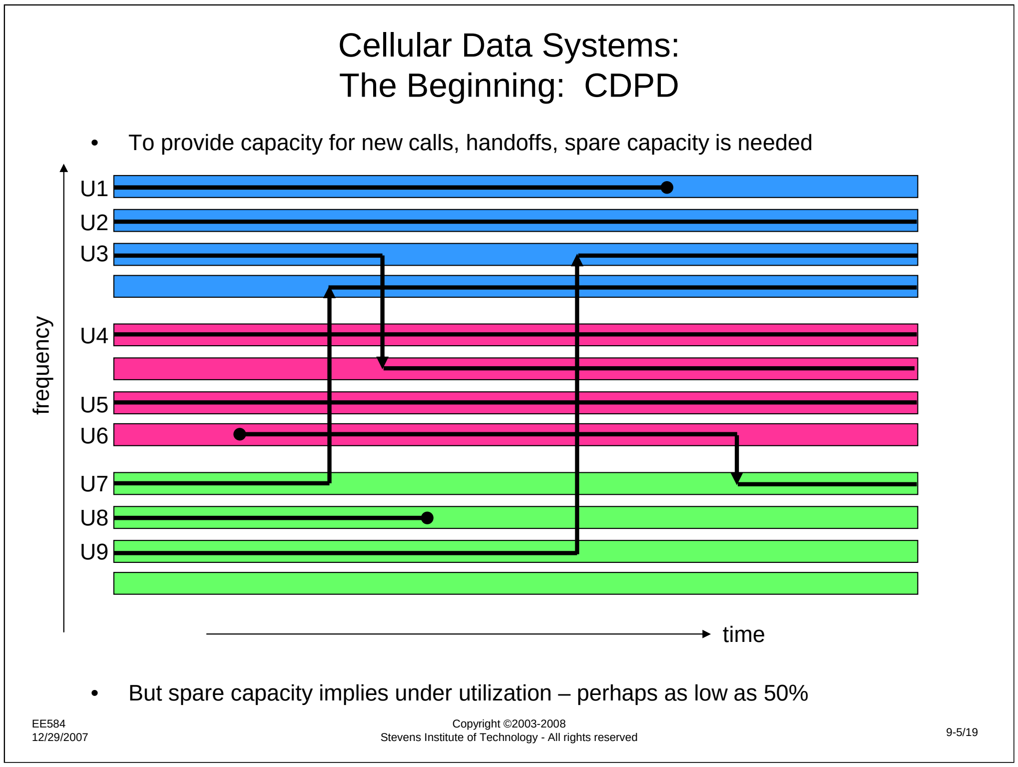
Cellular Data Systems: The Beginning: CDPD

- Consider three basestations, each with 4 frequencies available

EE584
12/29/2007

9-4/19

The first real wireless data service was CDPD. The original concept for this service was intriguing: in order to provide a low probability of dropped calls when handoffs occur, excess capacity is needed. But this excess capacity costs money and is only there to guarantee that there will be spare resources available when needed. How can the network be used at a higher average utilization without degrading voice quality? The concept of using the idle time on the spare channels to send packet data emerged. While a voice user cannot tolerate a delay in getting a dedicated channel, a packet data user is willing to buffer their data until capacity is available to get lower cost services.



Cellular Data Systems: The Beginning: CDPD

- To provide capacity for new calls, handoffs, spare capacity is needed

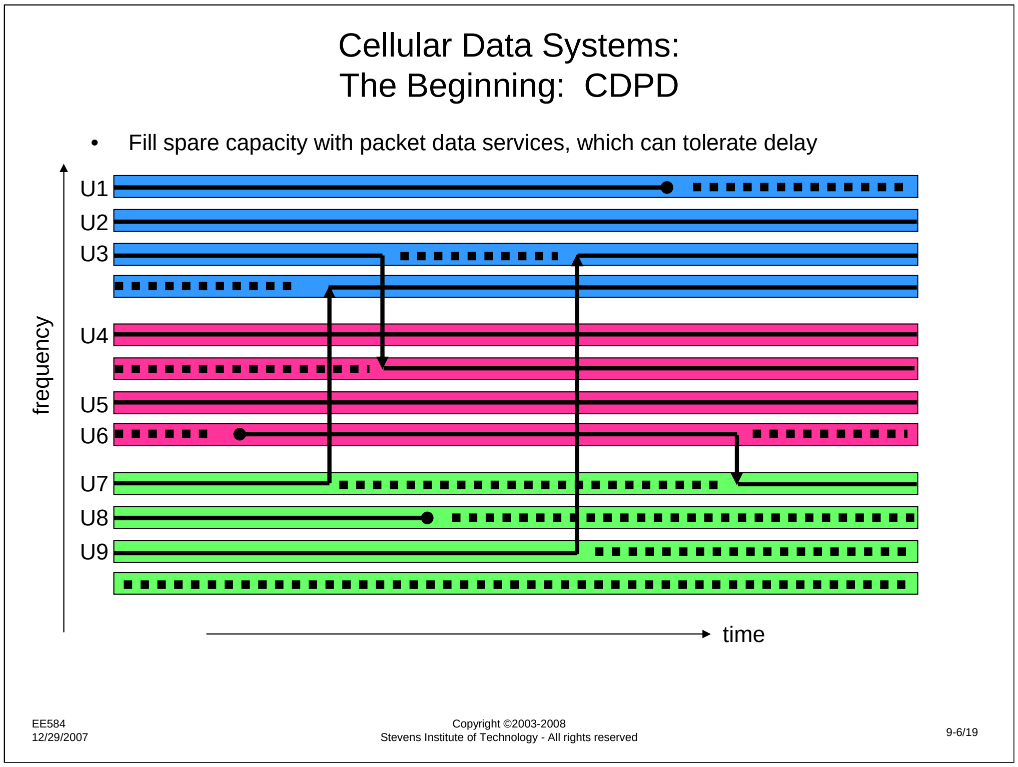
- But spare capacity implies under utilization – perhaps as low as 50%

EE584
12/29/2007

9-5/19

The diagram above illustrates a representative deployment. Here, there are three base stations, each with 4 frequencies available. A number of users start and end their calls at random times, and move from one location to another at random times, thus requiring handoffs. Examine three users: U1, U3, and U6. U1 has a call in progress at the beginning of the time interval illustrated above, but ends their call during the interval. After they end their call, the channel capacity is unused. U3 has a call in progress at the beginning of the interval, but needs to be handed off in the middle of the interval. Their channel capacity on the first base station is unused after the handoff and the channel they are handed off to must be idle when they arrive, so it is unused before their arrival. Finally, U6 starts their call in the middle of the interval we are examining. Their channel had to be unused before they started their call.

As you can see, there is a lot of capacity that is unused to allow the new calls and handoffs. There have been studies of cellular usage that suggest that 50% of the system capacity may be unused for reasonable levels of call blocking.



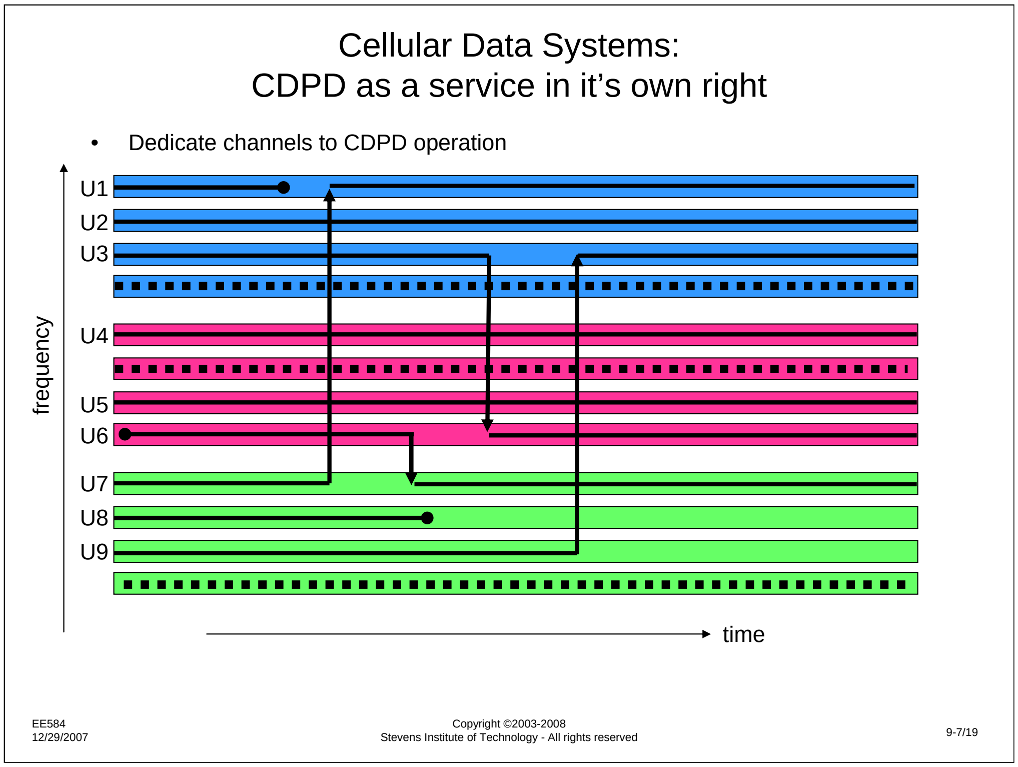
Cellular Data Systems: The Beginning: CDPD

- Fill spare capacity with packet data services, which can tolerate delay

EE584
12/29/2007

9-6/19

With CDPD, the unused time could be filled with data packets – if a brief interval is available, packets can be sent. If all the capacity is filled, the packet data users' traffic waits for available capacity.



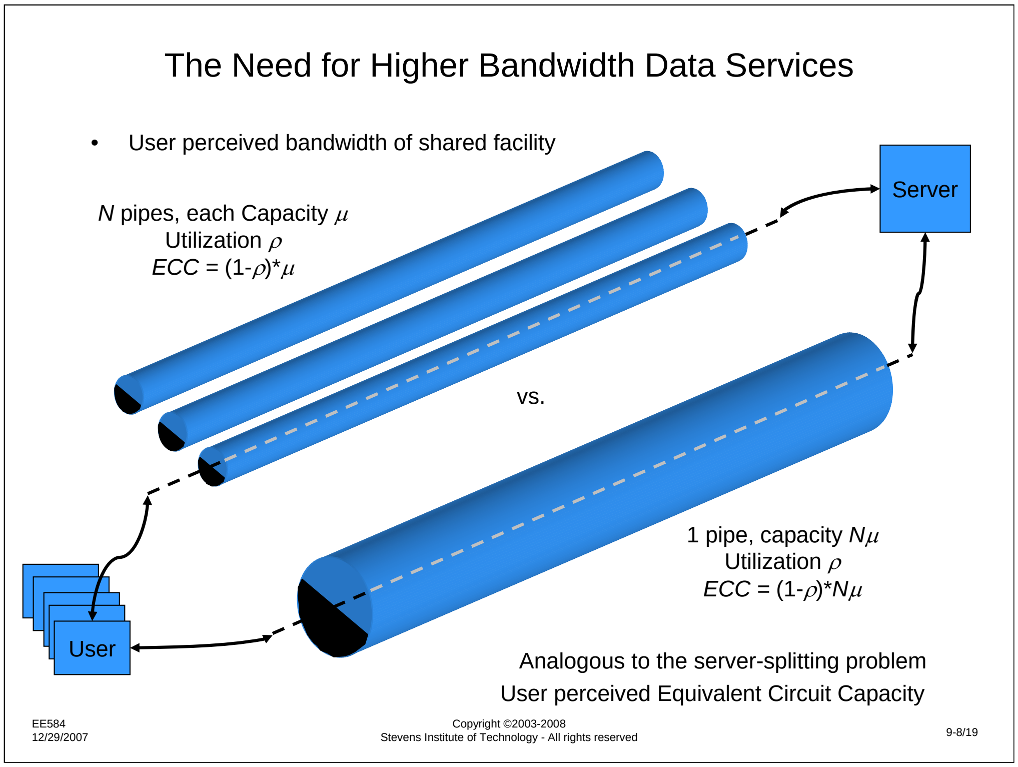
Cellular Data Systems: CDPD as a service in it's own right

- Dedicate channels to CDPD operation

EE584
12/29/2007

9-7/19

Of course, as data services are offered, and users find them useful, additional demand is created. The CDPD system that offered peak data rates of 19.2 kb/s in the blank periods of voice usage evolved until dedicated CDPD channels needed to be provided. Services like PalmNet, Sierra, and others have grown in popularity, despite the low capacity networks. Applications like tracking over-the-road trucking locations, parcel tracking, email, and others have thrived and are demanding more capacity.



The Need for Higher Bandwidth Data Services

- User perceived bandwidth of shared facility

N pipes, each Capacity μ
Utilization ρ
ECC = $(1-\rho)*\mu$

vs.

1 pipe, capacity $N\mu$
Utilization ρ
ECC = $(1-\rho)*N\mu$

Analogous to the server-splitting problem

User perceived Equivalent Circuit Capacity

EE584
12/29/2007

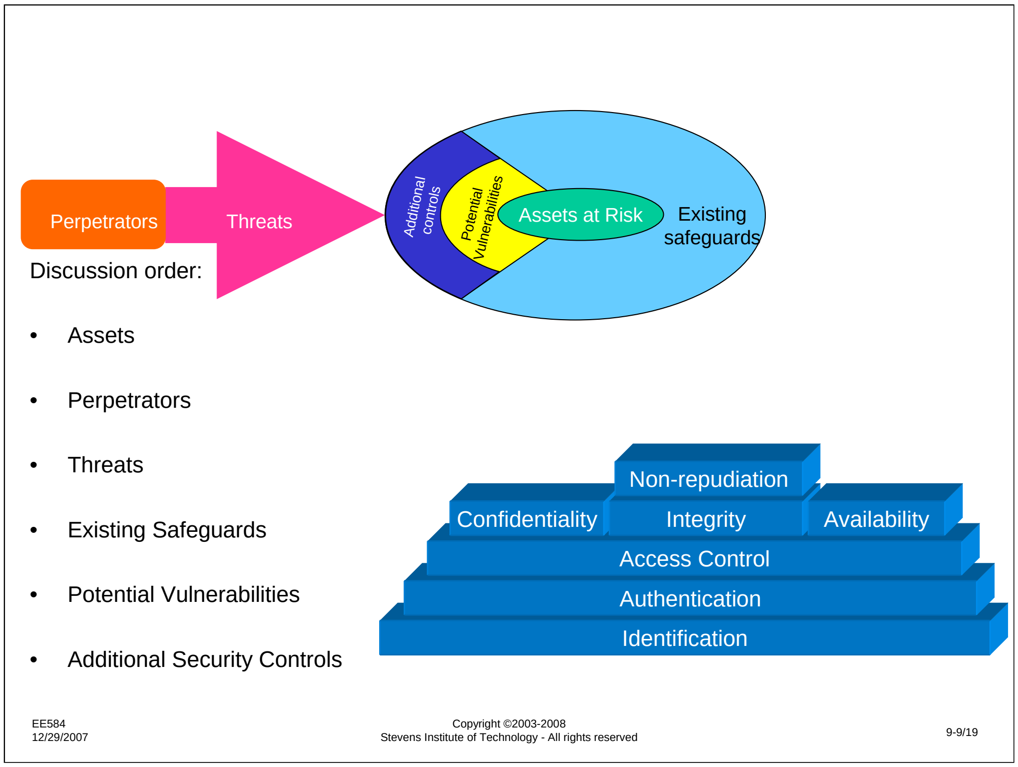
9-8/19

Which leads to this discussion of why we might want larger pipes and higher capacity services. Other than the sheer demand for more capacity, there are other interesting reasons to consider higher capacity data services.

One of my colleagues at AT&T Labs/Bell Labs (N. Shankaranarayanan) did some interesting studies to try to determine the user perception of wireless shared data networks. His question was: If users share a channel, what is their perception of the channel capacity? His results were very interesting, but very easy to understand, after the fact: if users are sharing a circuit, each feels that they have a dedicated equivalent circuit capacity equal to the unutilized capacity of the shared circuit. This is equivalent to a classic problem in queuing systems and computer systems called the server splitting problem. To get the best performance for the users, the total system capacity should be aggregated and distributed among all the users. For the wireless data user, this means that sharing a 19.2 kb/s circuit, with an average utilization of 50% feels like having a dedicated 9.6 kb/s circuit. On the other hand, if a large number of users were aggregated together and were sharing a 10 Mb/s channel, with the same 50% average utilization, it would seem to each of them that they had a dedicated 5 Mb/s channel. In each case, the user perceives the total unutilized capacity of the channel.

So this is the user draw of 3G and 4G – make the overall pipe bigger, and it gives all the users the perceived access to a high capacity channel. The draw for the system provider is that they can run the higher capacity system at a higher level of utilization and still make the users feel that they are getting access to a higher system capacity. (A 2 Mb/s pipe at 50% utilization feels like a 1 Mb/s dedicated channel, while a 10 Mb/s pipe at 80% utilization feels like a 2 Mb/s dedicated channel – and the economics of 80% utilization are much more desirable to the operator than 50% utilization)

But there is a security downside to this – fewer large pipes mean more single points of failure and bigger targets for attack.



Discussion order:

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

EE584
12/29/2007

9-9/19

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?

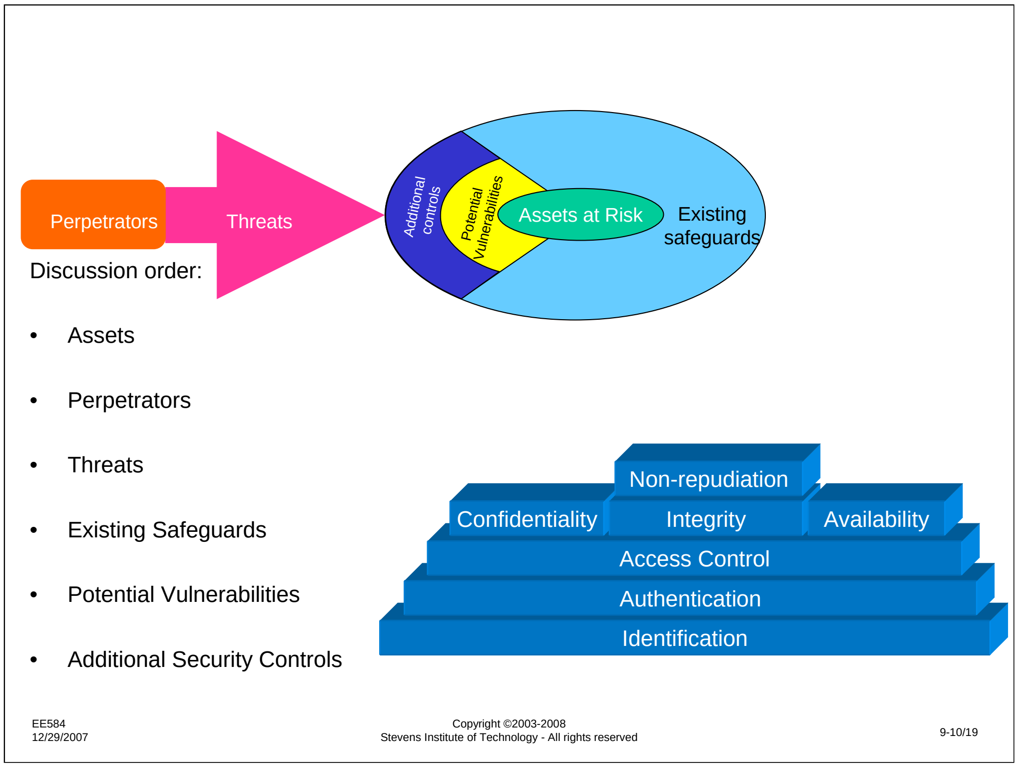
Threats: What mischief can you get into? How would you do it?

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.



Discussion order:

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

EE584
12/29/2007

9-10/19

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?

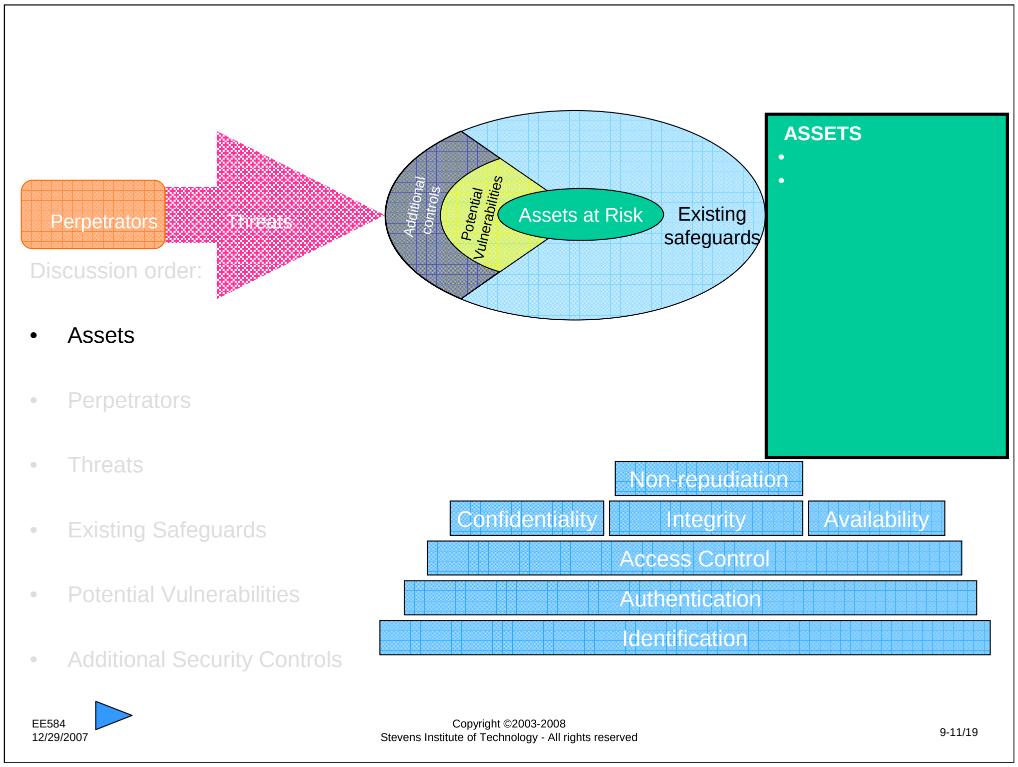
Threats: How might someone try to attack your system?

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.



Perpetrators
Threats
Additional controls
Potential Vulnerabilities
Assets at Risk
Existing safeguards

ASSETS
-
-

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

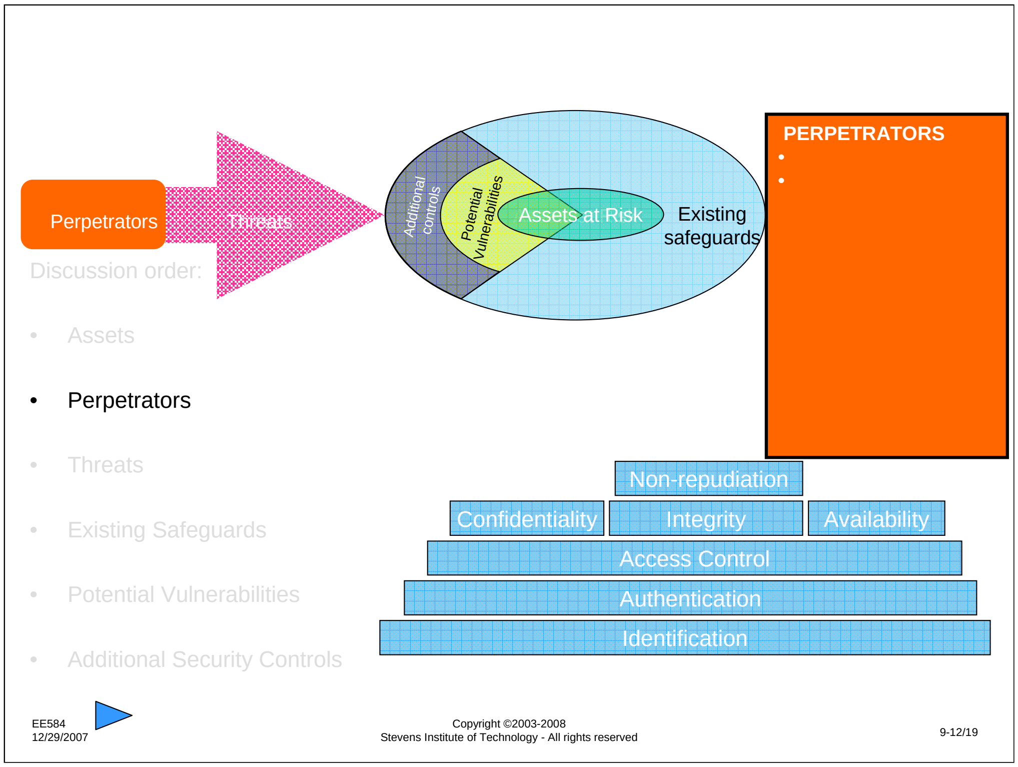
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

9-11/19

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.



PERPETRATORS

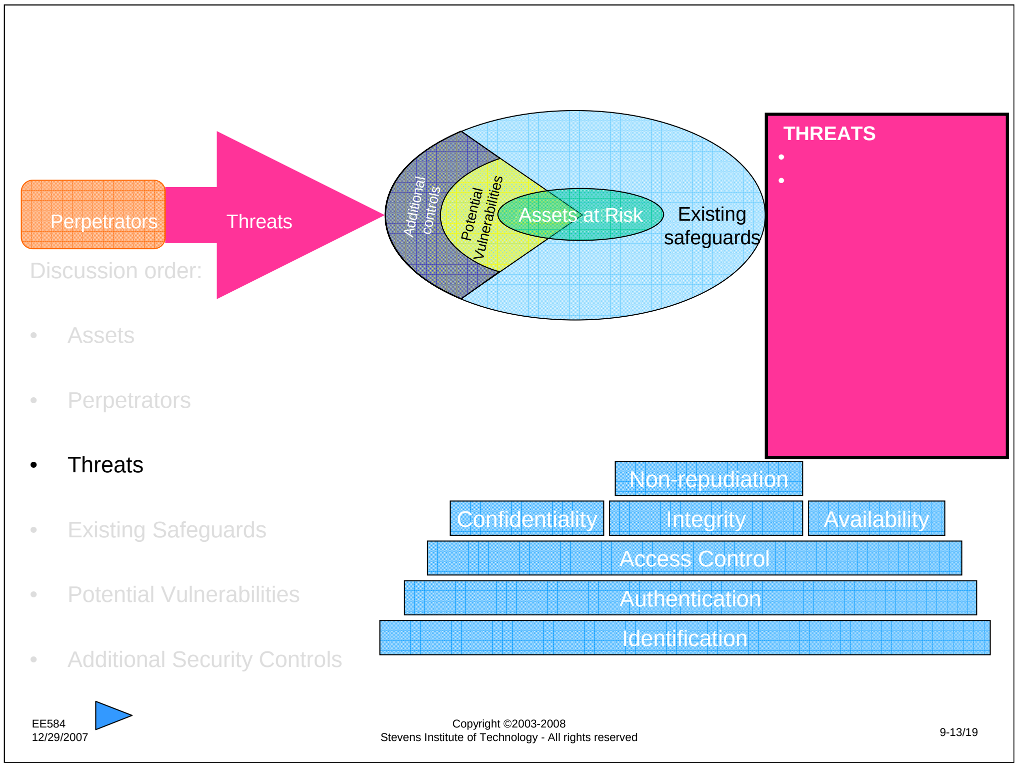
-
-

Discussion order:

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

EE584
12/29/2007

9-12/19



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

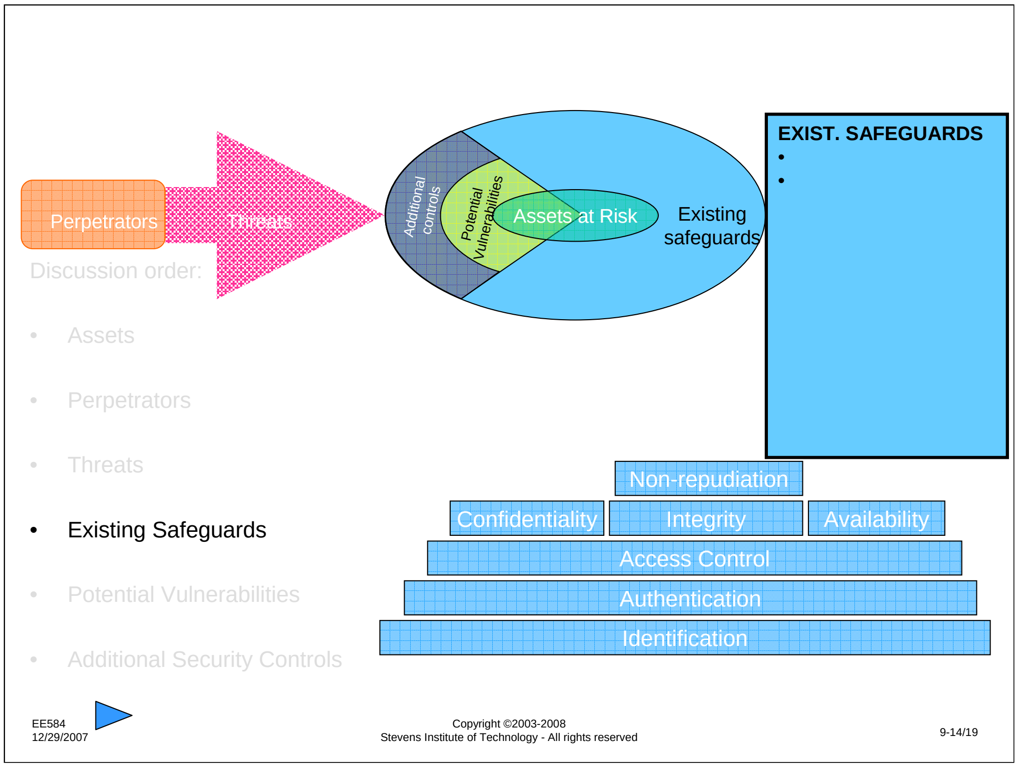
Confidentiality	Integrity	Availability

Access Control

Authentication

Identification

EE584
12/29/2007

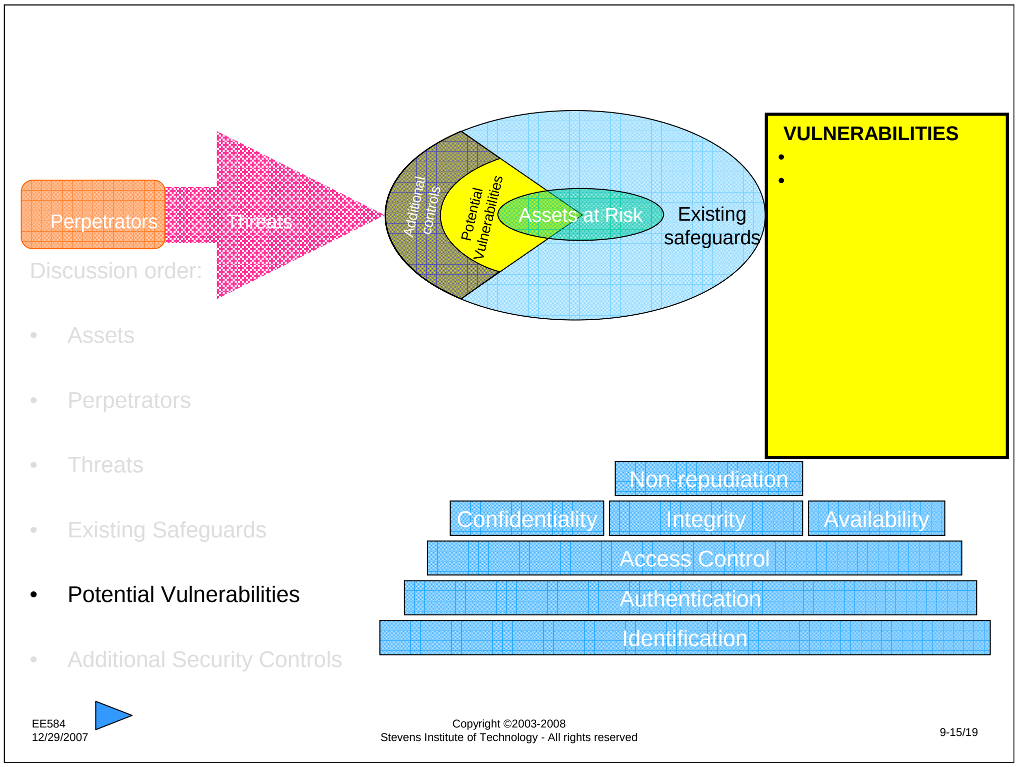


EXIST. SAFEGUARDS

-
-

Discussion order:

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



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

VULNERABILITIES

-
-

Non-repudiation

Confidentiality | Integrity | Availability

Access Control

Authentication

Identification

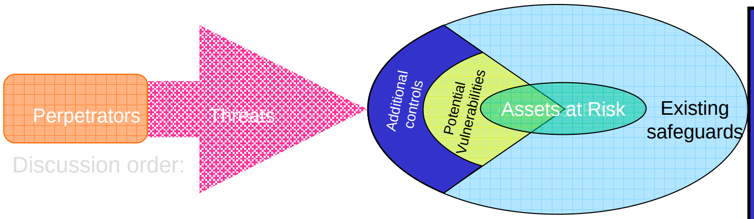
Discussion order:

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

EE584
12/29/2007

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

9-15/19

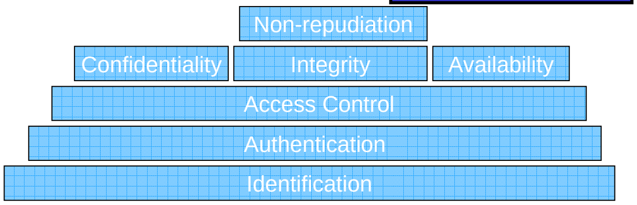


ADD'L CONTROLS

-
-

Discussion order:

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



ASSETS

•

•

PERPETRATORS

•

•

THREATS

•

•

EXIST. SAFEGUARDS

•

•

VULNERABILITIES

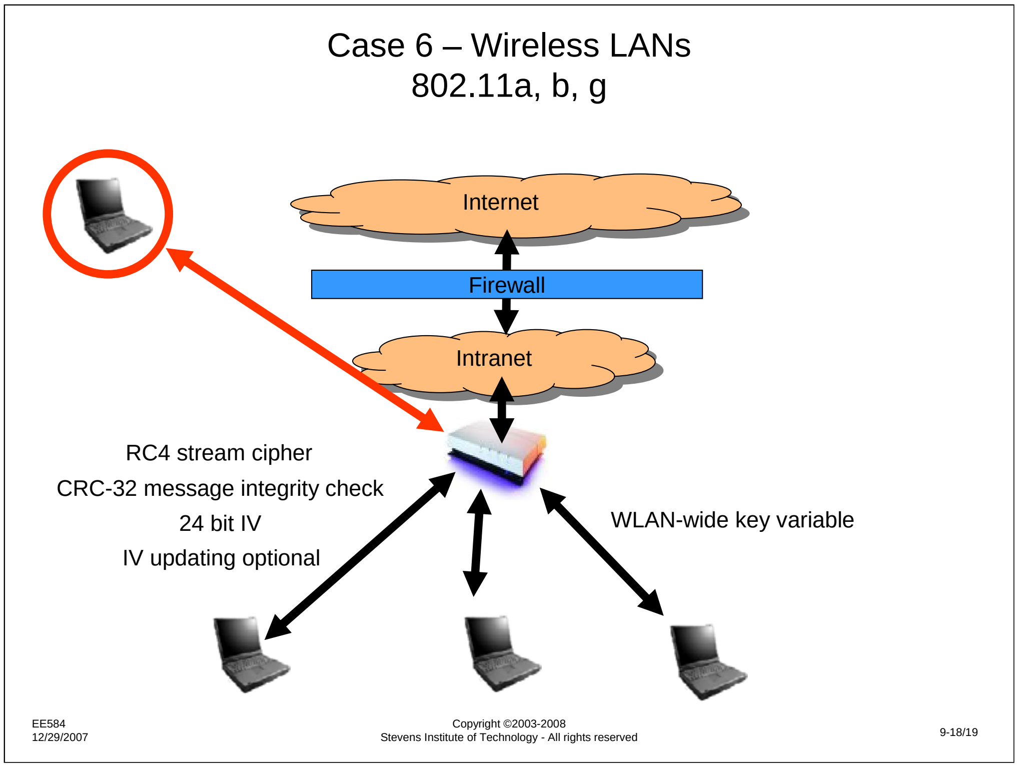
•

•

ADD’L CONTROLS

•

•



Case 6 – Wireless LANs 802.11a, b, g

Internet

Firewall

Intranet

RC4 stream cipher

CRC-32 message integrity check

24 bit IV

IV updating optional

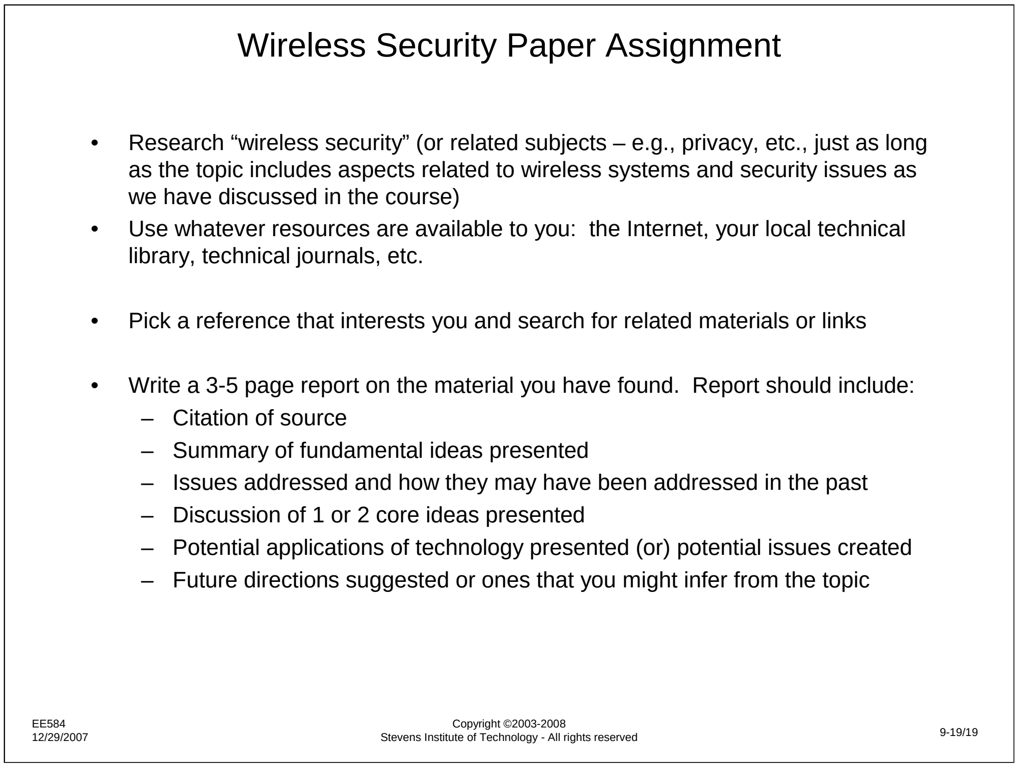
WLAN-wide key variable

EE584
12/29/2007

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

9-18/19

Next week, we will look at the security of wireless local area networks, like 802.11a, b or g. One of the terms you should research for next week's discussion is WEP (Wired Equivalent Privacy)



Wireless Security Paper Assignment

- Research “wireless security” (or related subjects – e.g., privacy, etc., just as long as the topic includes aspects related to wireless systems and security issues as we have discussed in the course)
- Use whatever resources are available to you: the Internet, your local technical library, technical journals, etc.
- Pick a reference that interests you and search for related materials or links
- Write a 3-5 page report on the material you have found. Report should include:
  - Citation of source
  - Summary of fundamental ideas presented
  - Issues addressed and how they may have been addressed in the past
  - Discussion of 1 or 2 core ideas presented
  - Potential applications of technology presented (or) potential issues created
  - Future directions suggested or ones that you might infer from the topic

EE584
12/29/2007

9-19/19

This being Week 9, it is time for the assignment of the third paper. This one is on the general topic of wireless security. As before, the paper is due in two weeks – during Week 11. The overall process is the same, just the potential references are different. For this paper, any topic in wireless security is acceptable and any source you want to use is acceptable. Just make sure you cite the source of your material.