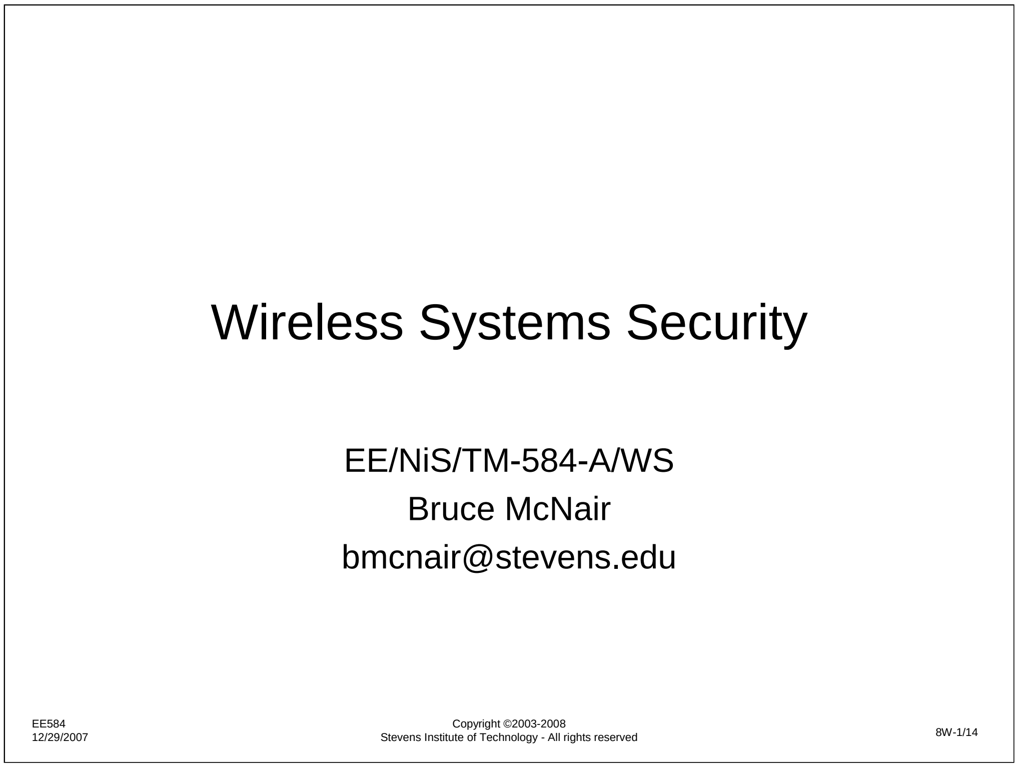
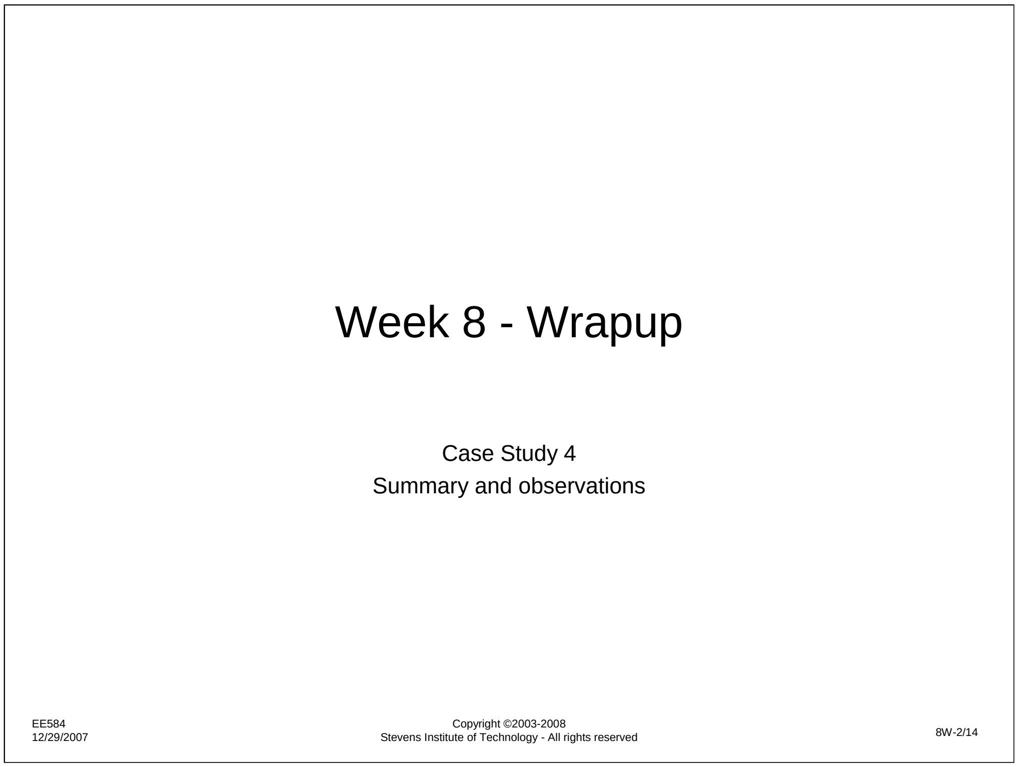


Wireless Systems Security

EE/NiS/TM-584-A/WS
Bruce McNair
bmcnair@stevens.edu



Week 8 - Wrapup

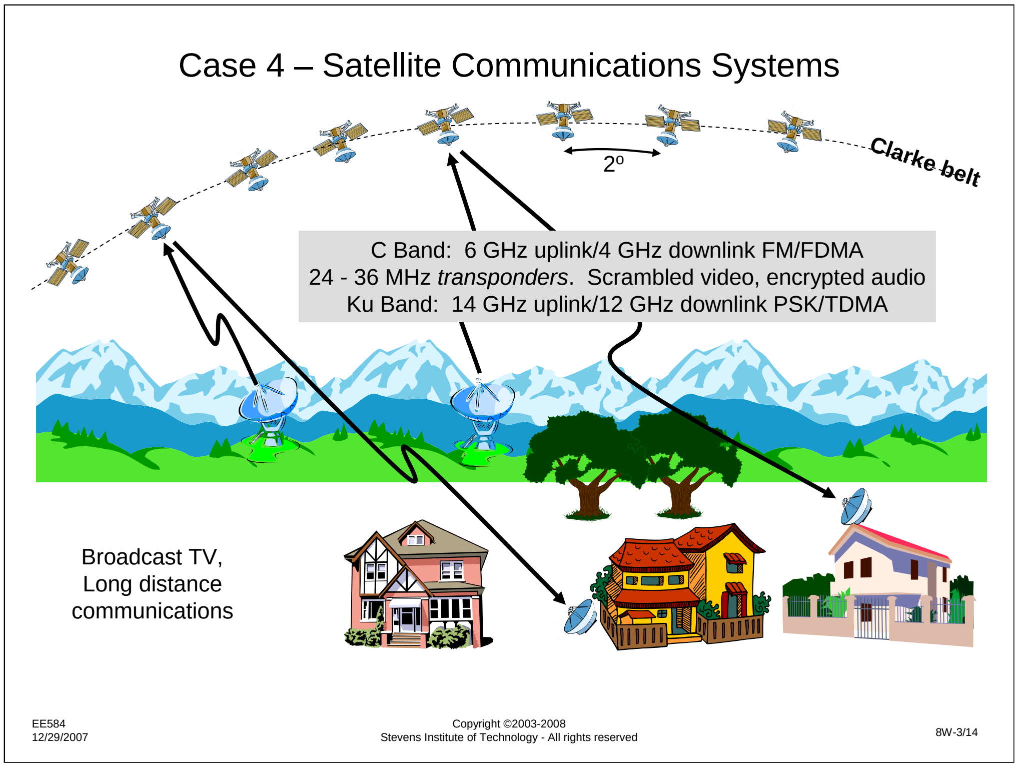
Case Study 4

Summary and observations

EE584
12/29/2007

8W-2/14

At this point, you have completed the discussions for the fourth case study. I wanted to make some observations about the system we have assessed and summarize the assessment. For the later, I am using assessment results from previous groups who have taken this class. I will add your assessment results to future versions of this class.



Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

Broadcast TV,
Long distance
communications

EE584
12/29/2007

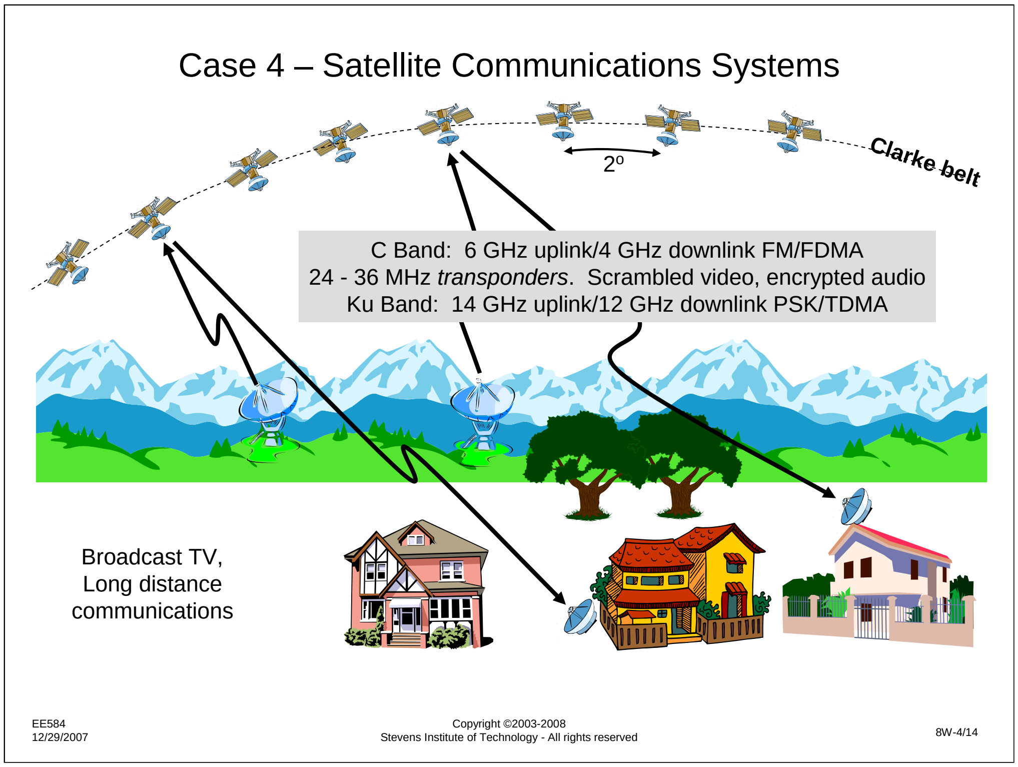
8W-3/14

There are a few reasons why I picked satellite communications systems for the fourth assessment. For one, the issues in a system that is intended primarily for entertainment are very different than the systems we have discussed before. While the other systems may have been driven by confidentiality of the transmissions to protect secret information, in this case, the information is still protected to keep unauthorized users from accessing it. However, this must be done in a context where a very large number of users are allowed to access the information. It is not so much the particular content, because in most cases it is information that has been previously opened for public disclosure. The issue here is that the satellite bandwidth is being paid for by the company who is licensing the distribution of content. They want to be sure they are reimbursed for their content. Theft of service, even of information that might be otherwise available is the issue.

I also picked this case because there have been lots of documented attacks against the confidentiality of satellite service. I'll go into the details on the next slides. These are not academic questions of could the service be compromised – it has been.

Unlike some of the other wireless services, where access is only possible over relatively limited areas, perhaps totaling dozens to hundreds of square miles, satellite communications are inherently wide area broadcasts. A satellite that covers the entire continental US has a coverage area of millions of square miles. There are two sides to this: monitoring can occur from anywhere the satellite signal is transmitted to; interference with the satellite uplink can occur from anywhere the satellite could receive a signal from.

Finally, there is the issue of protection of the satellite itself. A satellite owner spends many millions of dollars in having the satellite built, putting it in orbit, and operating the satellite for its useful lifetime. I don't know the total cost of ownership, but I wouldn't be surprised to find it might be close to a billion dollars. With this magnitude of investment, the satellite, as an asset in its own right, is more important than any comparable piece of any of the systems we have discussed. This means that the satellite operations themselves must be protected.



Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

Broadcast TV,
Long distance
communications

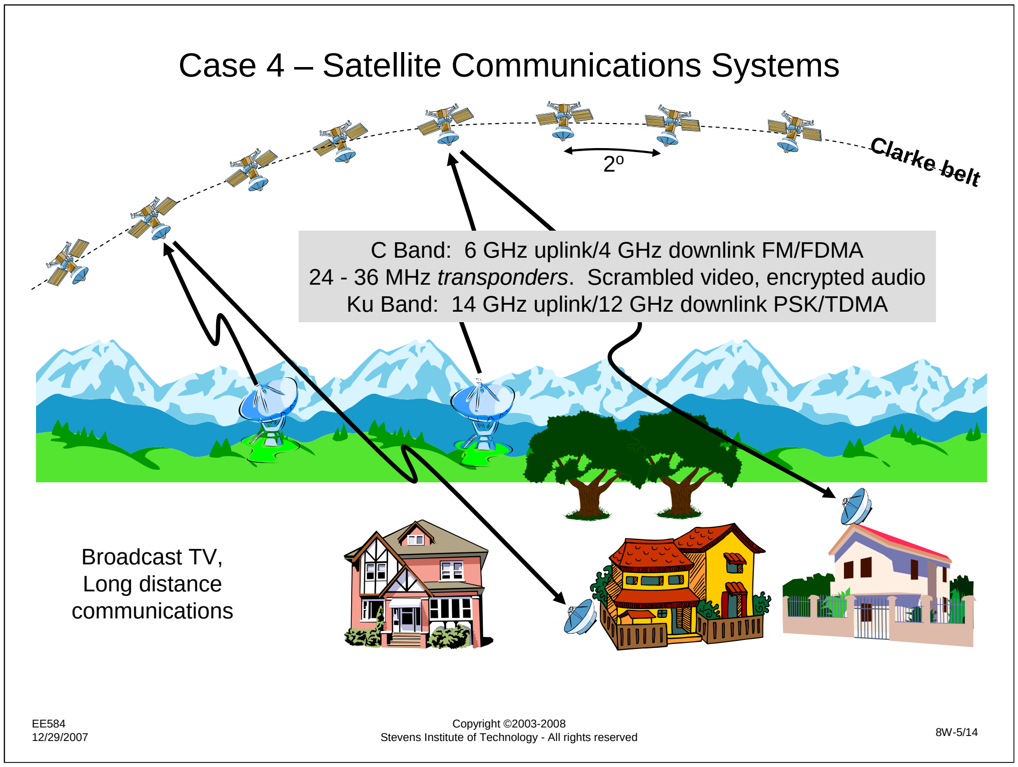
EE584
12/29/2007

8W-4/14

Let’s talk about a couple of real attacks against satellite communications systems.

First, the issue of theft of service. Satellite services like Home Box Office (HBO) purchase the rights to broadcast entertainment content to certain markets. A movie that has been shown in theaters in the US a year or two ago, might be available for HBO to broadcast. However, their rights are limited to, perhaps, the US. The reason for this is that the movie production company that owns the movie is selling seats in theaters in other countries long after the movie closed in the US markets. If someone in a Caribbean country, for instance, were able to receive the signal as part of a monthly HBO satellite subscription of $10, why would they spend $5 per ticket to bring their family of 4 to a theater to see the movie that was just released? Since many Caribbean islands are not that far from Florida, where HBO would certainly want to be able to broadcast their US programming, it is very likely that satellite receivers in, for instance, the Bahamas, would be capable of receiving strong signals. This is the reason why HBO must scramble their programming and why a Caribbean attacker might be motivated to figure out how to descramble the signal. I use the example of a Caribbean attacker, because historically, this is where most of the attacks on satellite scrambling have actually come from.

How does satellite TV scrambling work, and how does one go about attacking it? It would be ideal if the satellite video could be digitally encrypted, as the military encrypts voice signals. However, to digitally encrypt the analog video signal would require processing a wideband signal digitally, something that has not been practical or even possible until recently. Instead, the video scrambling systems used in C-band satellite merely distort the signal to make it unusable for entertainment purposes. This is done by eliminating the horizontal synchronization signal from the video, causing the picture to tear from side to side. The audio is digitally encrypted, easy to do because of its lower bandwidth. While one might be able to descramble the video, watching ***most*** movies without the sound causes them to lose most of their entertainment value.



Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

Broadcast TV,
Long distance
communications

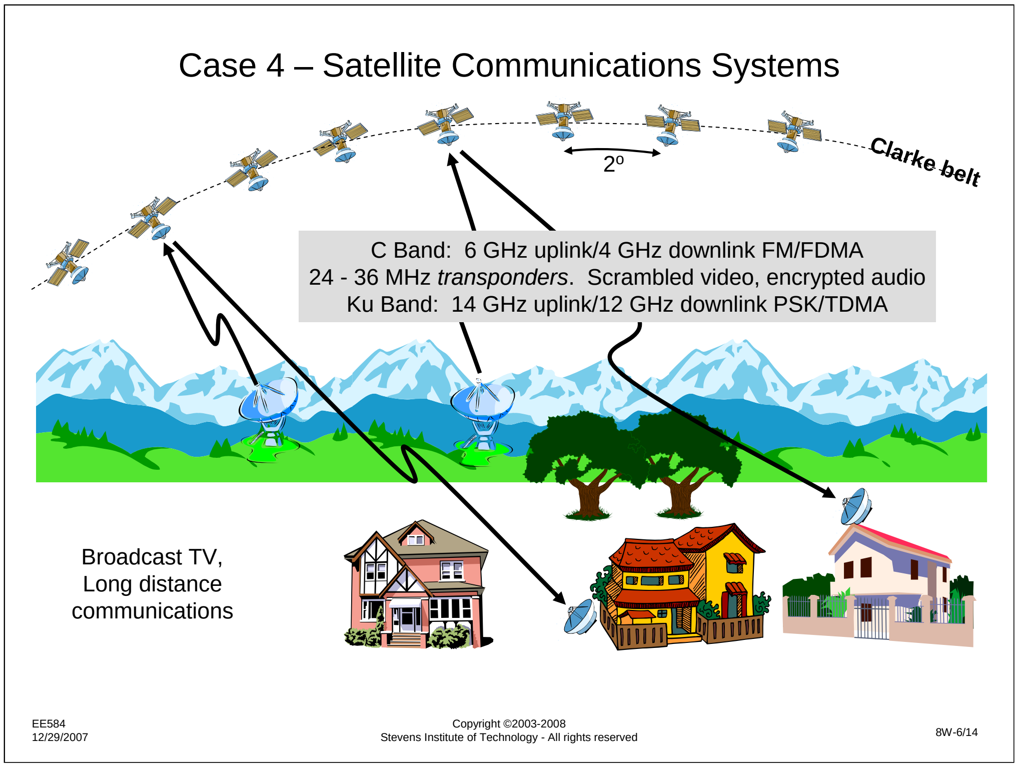
EE584
12/29/2007

8W-5/14

What about jamming a satellite transmission? It obviously isn't going to be easy to jam the downlink. The jammer would have to be somewhere near the satellite for all the ground stations to be able to even see the jammer. On the other hand, the satellite is looking down at the Earth. A jammer with sufficient power could capture the uplink and put their own programming on the satellite. Again, this is a real issue that we have an existence proof for. When HBO first started operating, they did not scramble their signal, since there were few individuals who had satellite receivers. The cable operators who were distributing HBO over their systems weren't likely to steal service, since they were regulated by the FCC and local communities. It was easier to pay for their subscriptions and pass the costs to their users. Shortly after HBO realized that motels, bars and other places where one receiver could feed multiple TV sets were routinely distributing their signals, they began scrambling and required users to subscribe to the services and buy descrambling equipment. Apparently annoyed by this new practice, a hacker generated an uplink signal that was stronger than HBO's uplink and, for a few hours, took over their system, transmitting messages about the hacker's opinion of HBO's management and business practices.

Considering that HBO's uplink is a high power transmitter with a large satellite antenna, it obviously took someone with comparable equipment to be able to take over the link. This, in itself, restricted the potential attack sites to a handful. Further, it turned out that the TV character generator used to create the messages had some easily identifiable characteristics, which enabled the FCC to identify the manufacturer. Putting the two items together enabled investigators to trace the pirate uplink to a rarely used uplink station in Ojai, California.

I mention this example for two reasons: first, it shows that satellite systems have been attacked; second, while CSI would be proud of the FCC's ability to track down the attacker, this is not to say that a more subtle attack might have been much more difficult to investigate and prosecute.



Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

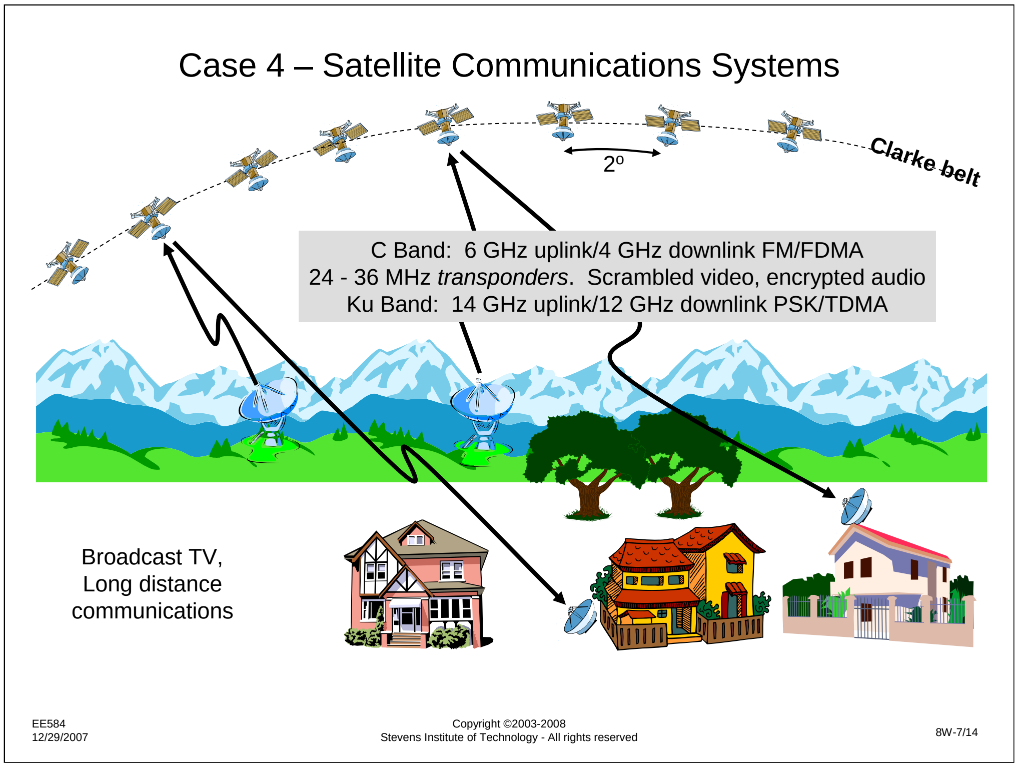
Broadcast TV,
Long distance
communications

EE584
12/29/2007

8W-6/14

“Station keeping” refers to the process of maintaining a satellite’s orbital position – to be useful, a satellite must maintain a fixed position, relative to a point on the Earth. If the Earth were perfectly spherical, there were no other gravitation forces acting on satellites (the two-body problem in orbital dynamics), the satellite were traveling through a absolute vacuum, and there were no other factors influencing the satellite orbit (e.g., the Earth had no magnetic field), keeping a satellite in the proper orbit would just be a matter of initially launching it, and leaving it alone. Unfortunately, several factors cause the satellite to drift. This drift is compensated for by firing small rockets to undo any movement or rotation of the satellite. These rockets require fuel which must be launched with the satellite and, like everything else that is launched, requires a lot of energy to lift the satellite 24000 miles into geostationary orbit. Thus, the station keeping ability of the satellite is an important asset, if the satellite is to be useful for the longest period of time.

Station keeping is managed from the ground station on a wireless control link. Again, there is an existence proof of this link being attacked and hackers taking the satellite for a “joy ride.” It was possible to detect the deviation of the satellite from its proper position and take back control of the link before a serious quantity of the station keeping fuel was expended, but this attack had the potential to seriously jeopardize the lifetime of the satellite.



Case 4 – Satellite Communications Systems

C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

Broadcast TV,
Long distance
communications

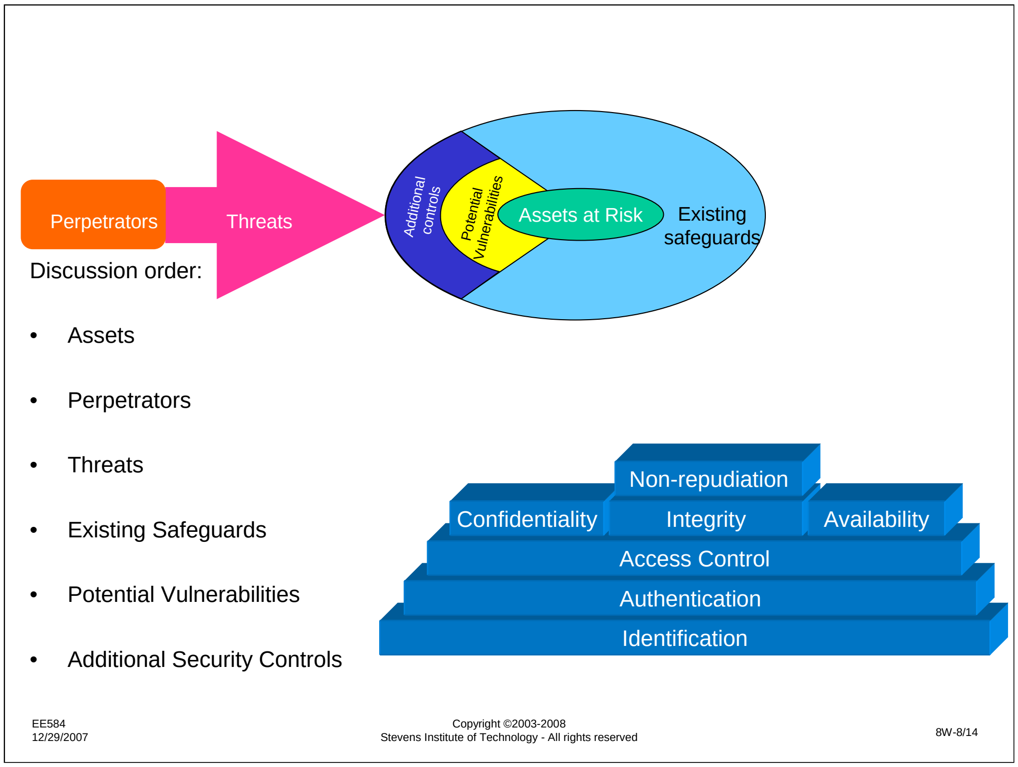
EE584
12/29/2007

8W-7/14

All of the attacks described above are real attacks that have actually occurred. This last exploit is theoretical, based on some real issues. It also has the potential to be nearly undetectable.

I had occasion to consult on the source of apparently ground-based interference degrading the performance of an Intelsat satellite used to provide a international data circuit. While we never resolved the source of the interference (it just went away one day), the investigation uncovered some interesting potential issues that I am mentioning here.

Realize that the satellite is really just a broadband repeater. Whatever it hears on its uplink is rebroadcast on its downlink. Normally, this is one of a small set of intended users. If the users are transmitting FDM or TDM signals, their signals will be appropriately distributed. The hypothetical issue here is, what if there is a spread spectrum transmission on the uplink of an otherwise TDM or FDM system? How would this signal appear to the other users and what influence would this signal have? As it turns out, a well-crafted spread spectrum signal should be hidden in the noise for fixed frequency users. Only a receiver with the proper spreading code would be able to detect the spread signal. On the other hand, the spread signal is adding a certain amount of power to the uplink signal, which will appear on the downlink signal as additional signal power and noise. In other words, a clever spread spectrum user would look to the valid users as if the satellite link were slightly degraded – maybe the satellite power has dropped off a bit, or perhaps the antenna is slightly mispositioned. In other words, the spread spectrum user could conceivably freely use satellite transponders without detection by all but the most intense scrutiny.



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing 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

8W-8/14

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?

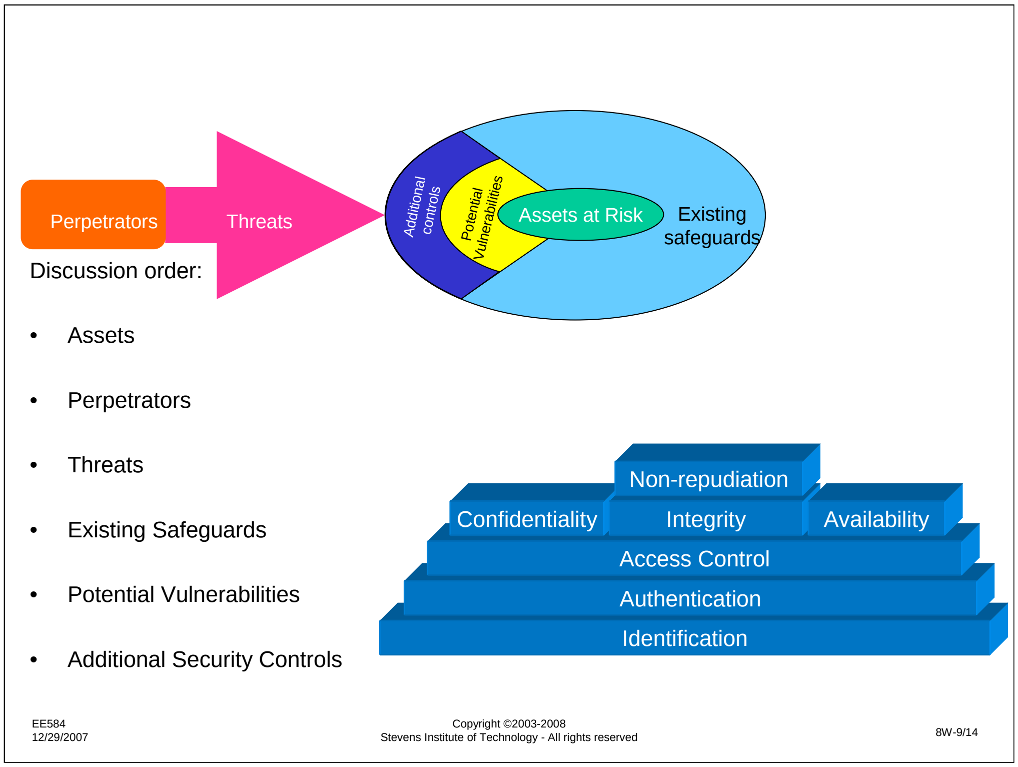
Threats: What mischief can you get into? How would you do it?

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.



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing 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

8W-9/14

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?

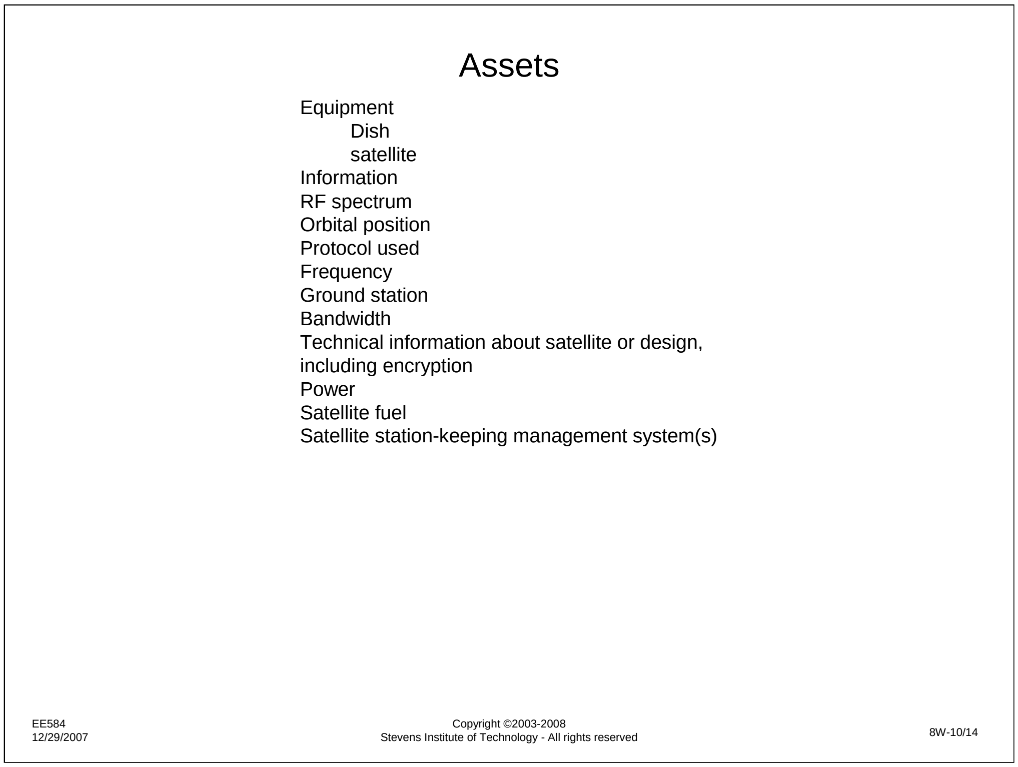
Threats: How might someone try to attack your system?

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.

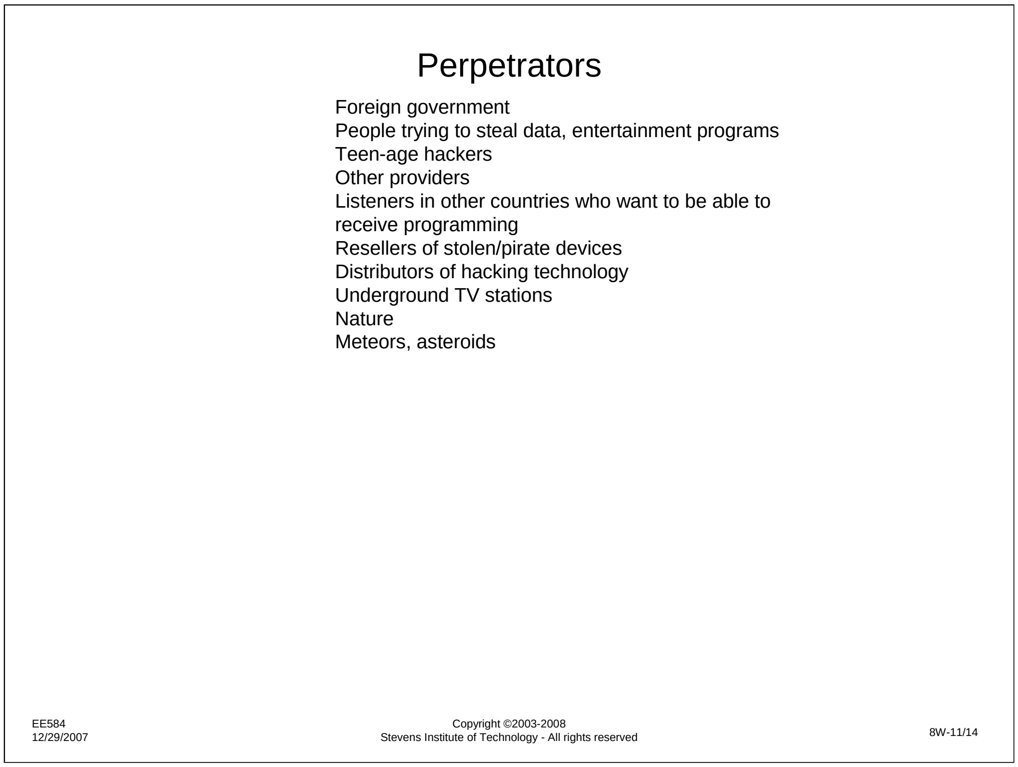


Assets

Equipment
- Dish
- satellite

Information
RF spectrum
Orbital position
Protocol used
Frequency
Ground station
Bandwidth
Technical information about satellite or design, including encryption
Power
Satellite fuel
Satellite station-keeping management system(s)

Listed above are a set of assets identified by other sections of this class. Not attempt has been made to filter or sort the concepts, so there may be redundancy between the different groups. Items in italics are those that were considered to be especially important.

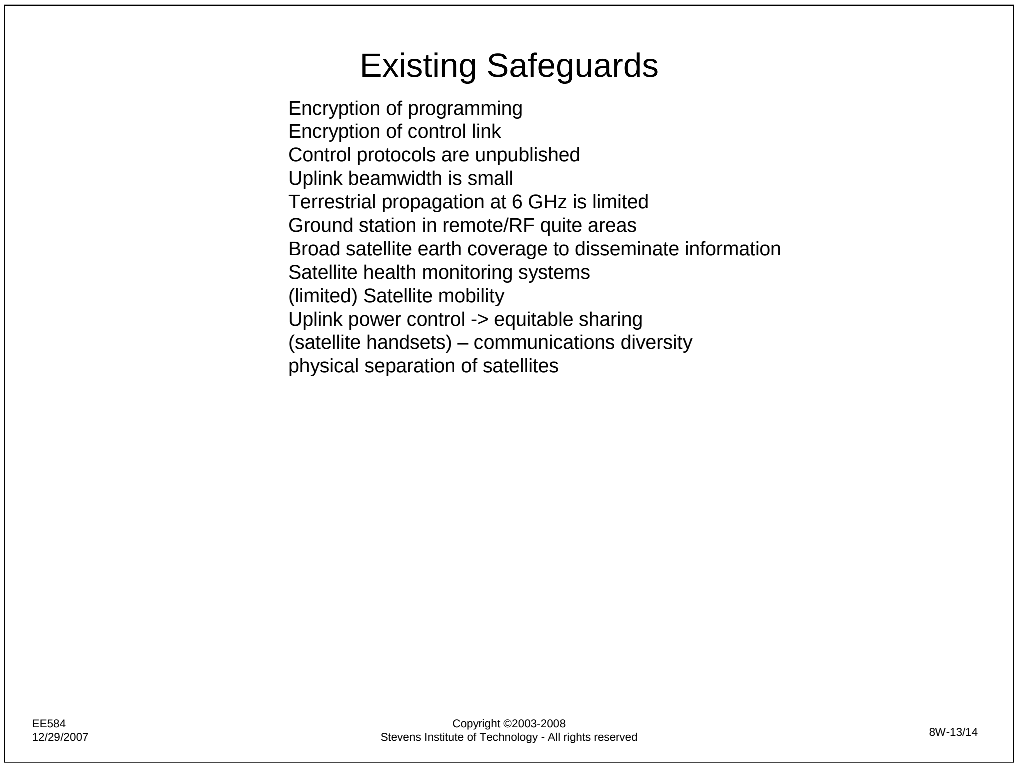


Perpetrators

Foreign government
People trying to steal data, entertainment programs
Teen-age hackers
Other providers
Listeners in other countries who want to be able to receive programming
Resellers of stolen/pirate devices
Distributors of hacking technology
Underground TV stations
Nature
Meteors, asteroids

Threats

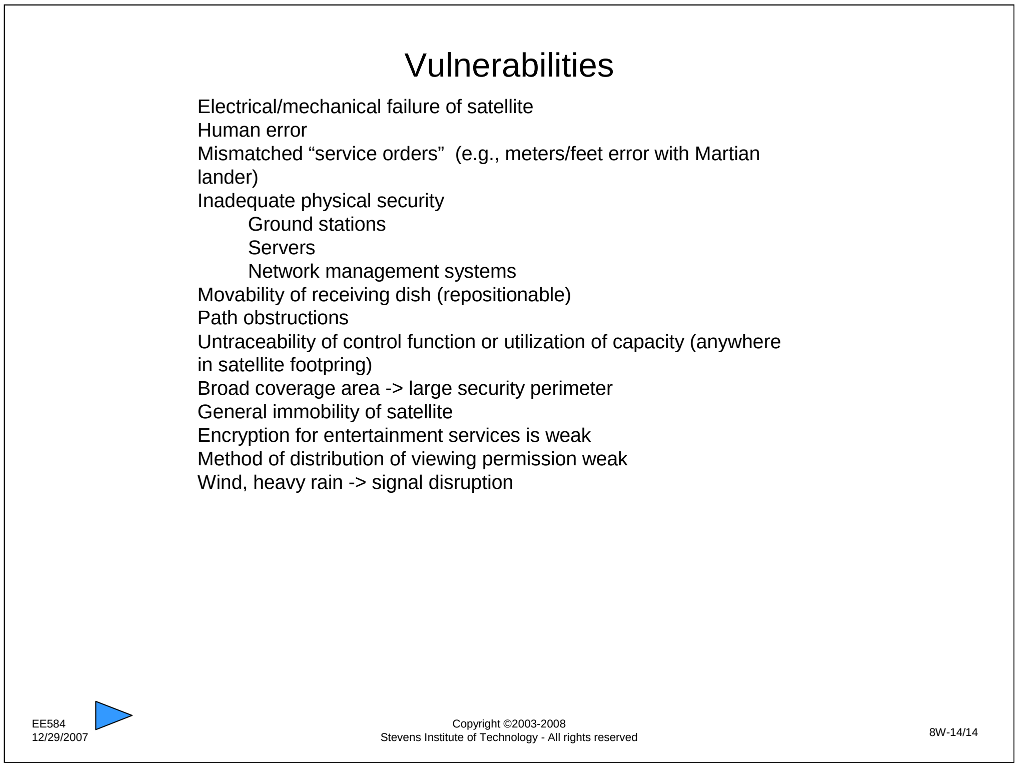
Physical destruction of uplink ground station
Orbital projectiles
Jamming
Hacker gets into satellite control system and unparks satellite, wasting fuel
Land-satellite projectiles
Guided energy weapons
Destruction of any part of system, including cables, can render system unusable
Jam downlink from aerial platform (e.g., balloon)
Intercept information
Special interest group (e.g., PETA) takes over uplink to broadcast their propaganda/announcements
Exploit sensitive information about system
Steal transponder bandwidth with spread-spectrum signal



Existing Safeguards

Encryption of programming
Encryption of control link
Control protocols are unpublished
Uplink beamwidth is small
Terrestrial propagation at 6 GHz is limited
Ground station in remote/RF quite areas
Broad satellite earth coverage to disseminate information
Satellite health monitoring systems
(limited) Satellite mobility
Uplink power control -> equitable sharing
(satellite handsets) – communications diversity
physical separation of satellites

Note: Some of these existing controls aren't actually existing controls, but are more additional controls.



Vulnerabilities

Electrical/mechanical failure of satellite
Human error
Mismatched “service orders” (e.g., meters/feet error with Martian lander)
Inadequate physical security
- Ground stations
- Servers
- Network management systems

Movability of receiving dish (repositionable)
Path obstructions
Untraceability of control function or utilization of capacity (anywhere in satellite footpring)
Broad coverage area -> large security perimeter
General immobility of satellite
Encryption for entertainment services is weak
Method of distribution of viewing permission weak
Wind, heavy rain -> signal disruption