Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

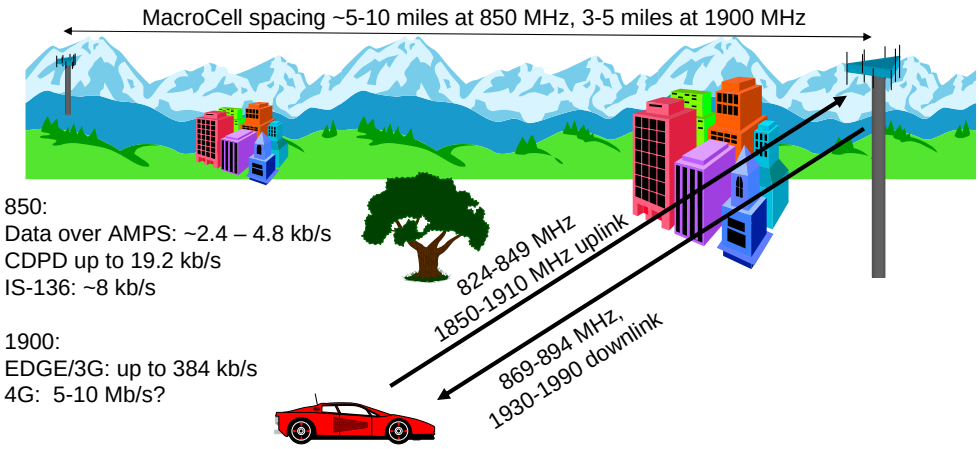
Week 9

Case Study 5
Summary and observations

At this point, you have completed the discussions for the fifth 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.

One student in one of the sections of this course made the observation that it is so much harder to defend than it is to attack – the defender has to cover all possible attacks, while the attacker only has to find one hole: Since it is so difficult to cover every potential hole, the defender must operate as efficiently as possible, and the only way to do this is to anticipate how the attacker might think, looking at the assets of the system and the barriers from the outside. This is exactly the point I want students in this class to come to, and why I spend so much time on assessments: you are forced to think like an attacker when you are assigned to a Red Team; you have probably never quite looked at a system in this way before; I could go over the issues in secure system design and the techniques to design securely, and I could highlight the particular issues of wireless systems, but I have found the assessment technique forces you to get engaged in the investigation, which seems to be a more effective teaching technique than others I have seen.

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?

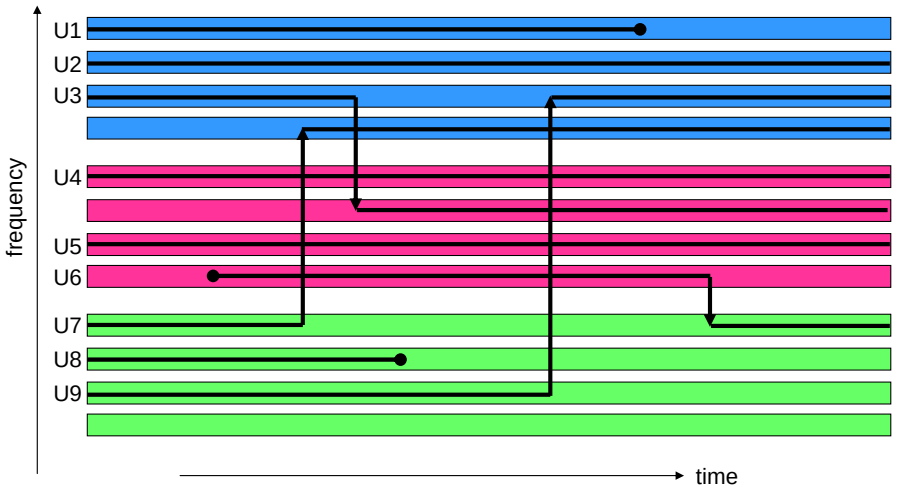
Previous assessments have included some systems for historical reasons and to put issues in perspective. Satellite communications, terrestrial microwave, military systems, etc., all have their unique issues, but the thing they have in common is that they are existing systems that have been in operation for several years. What is different about this case study is that we are discussing evolving systems. CDPD has only been available for a few years. EDGE and 3G are just now being deployed in many markets – it is not unlikely that for many areas of the country, these services cannot yet be ordered, while they are nearly entirely rolled out in nearby areas. Beyond this, 4G is still only a concept. We are not likely to see the first 4G systems for several years. So, this is actually a very appropriate time to be investigating security issues in the new data services these wireless service will provide.

One unique characteristic of evolving services is that one can never anticipate how the services will catch on or what new applications will be developed. The Internet started its explosive growth in the early 1990s. At that time, it was the confluence of widely available computing, a graphical user interface, and developments in data communications technology that fueled the growth, but it was the creation of a usable browser that sparked the development. That rapid evolution never anticipated some of the applications we now see as commonplace – email, streaming audio, file sharing, electronic commerce, etc.

In the same manner, we can't really be sure what will happen with the mobile wireless applications, but, just as someone who had been using email and ftp since the late 1970s might have predicted a 1991 Internet future that included some form of file sharing and email, it is probably safe to guess that the broadband wired applications of today will probably exist in some form when broadband wireless becomes ubiquitous. It is those applications and information asset exposures that we have to think about as we examine wide area wireless data services.

Cellular Data Systems: The Beginning: CDPD

- Consider three basestations, each with 4 frequencies available

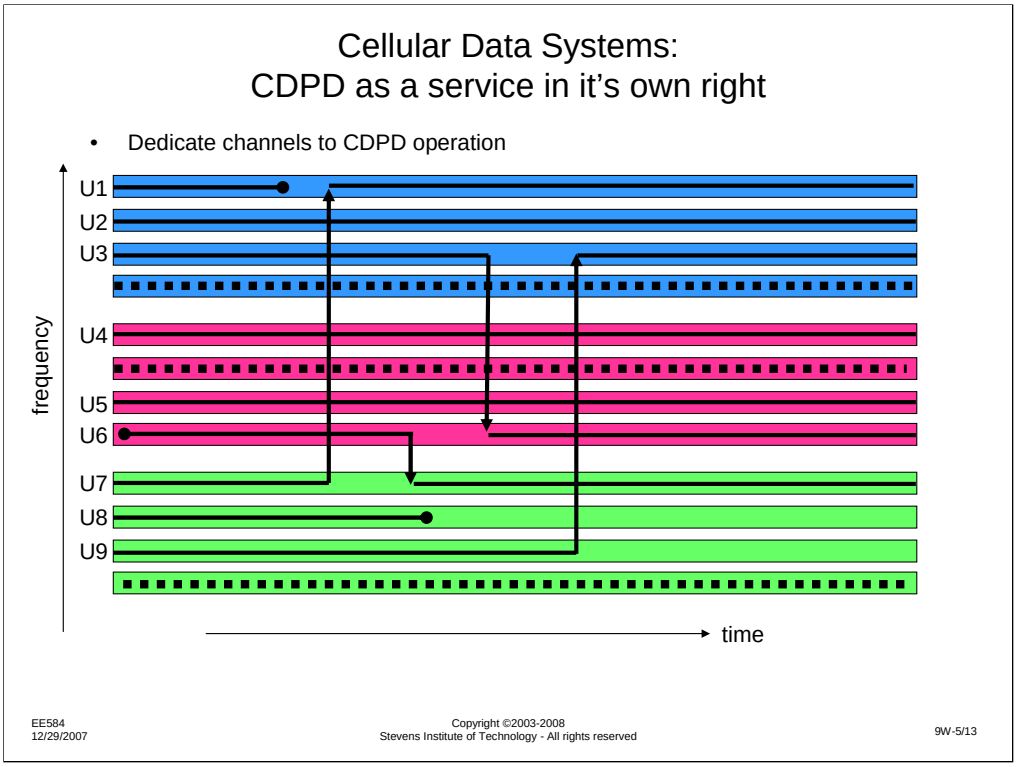


EE584
12/29/2007

9W-4/13

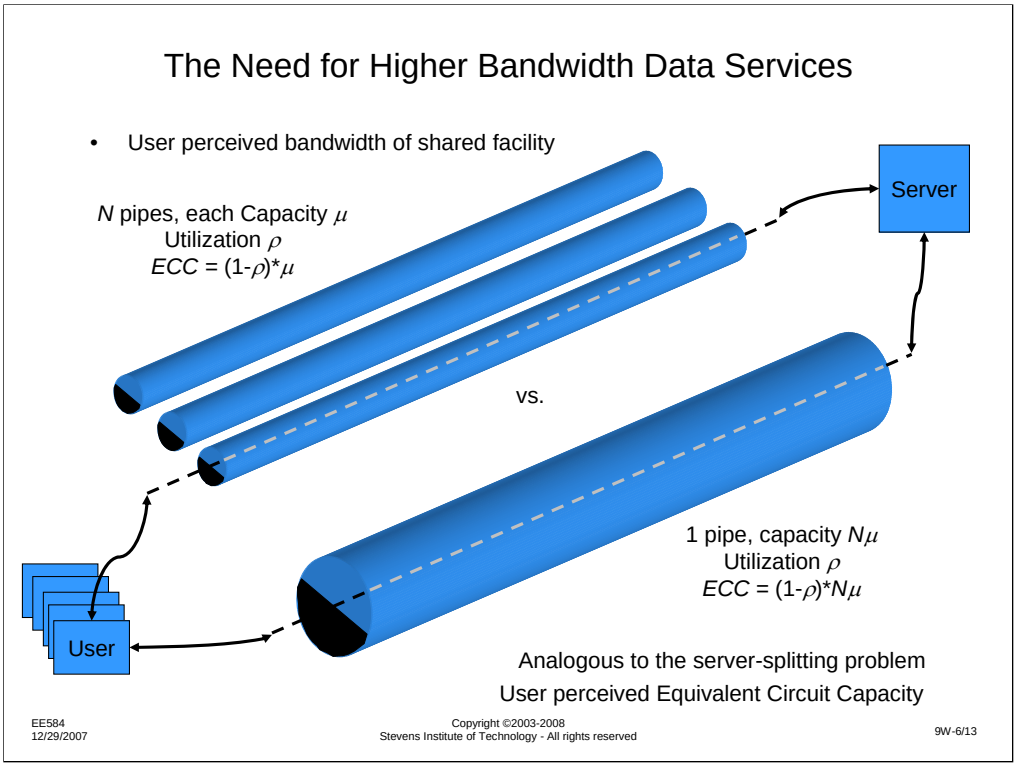
Let's look at a few of the applications that became enabled by the high-latency, low-bandwidth mobile data capabilities of basic CDPD: where might it be useful for me to be able to exchange small packets of information where the delay times aren't a bother. Extrapolating the email application, short messages (an alert, not a thesis) can be readily accommodated by CDPD. I was going to make an observation that email would never replace the spontaneous interactive conversations of a voice call, but then I thought of instant messaging, which gets pretty close. Mostly, email has eliminated the need for personal handwritten letters, substituting a 3 day latency with a 3 minute latency. Some other applications where messages are small and don't require immediate delivery are those where the message moves much faster than the physical object it is associated with – real-time parcel tracking is one important example of this. Without a way to signal delivery confirmation back to the sender, this capability isn't very useful. We now take for granted the ability to know a UPS or FedEx parcel has been delivered a few minutes after it has happened. Likewise, the owner of a fleet of trucks can now get immediate updates on any truck's position with GPS vehicle tracking and CDPD messaging. So much for the driver taking a nap in the middle of the day.

As we start to think of these types of applications, we can start to consider new assets – the location of the delivery van, the status of a diamond shipment, etc.

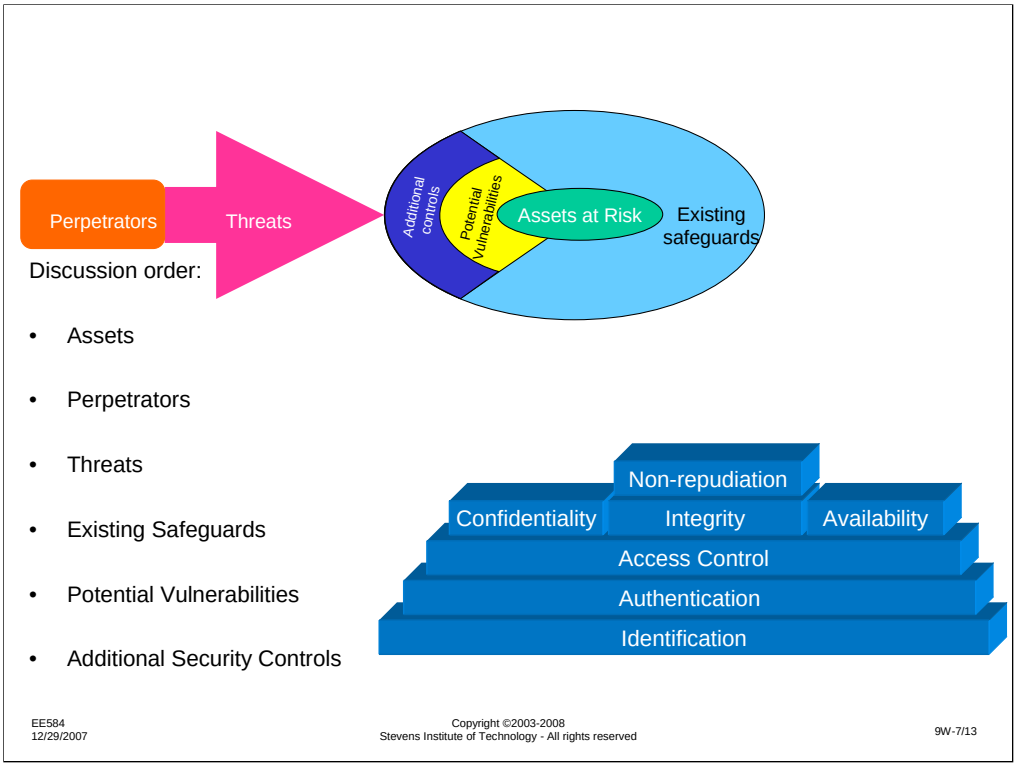


Like any other service, if it works well and fits a need, demand will grow, and the service will need to be enhanced to meet the additional need. Which immediately leads to the next level of threat – attackers are not as likely to attack an obscure target as a high profile one, there is no percentage in it for them. That is why the Macintosh and linux platforms have been relatively unscathed recently from all the virus and worm activity, and it is also the reason I use Netscape as a browser (besides the fact that I am used to its features and quirks, Internet Explorer is too inviting a target for the hackers – why bother with Netscape that has less than 25% of the share?).

So, we have to deal with this perverse set of motivations when considering wireless system security – useful capabilities are ones that we are likely to become dependent on, increasing the likelihood that an attack will make them unavailable.



Ultimately, this reasoning leads us to develop a few really large bandwidth pipes, creating the smallest number of points of failure. Hopefully, this will cause the facilities to be recognized as the critical infrastructure they are, leading to the deployment of security controls to protect them.



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?

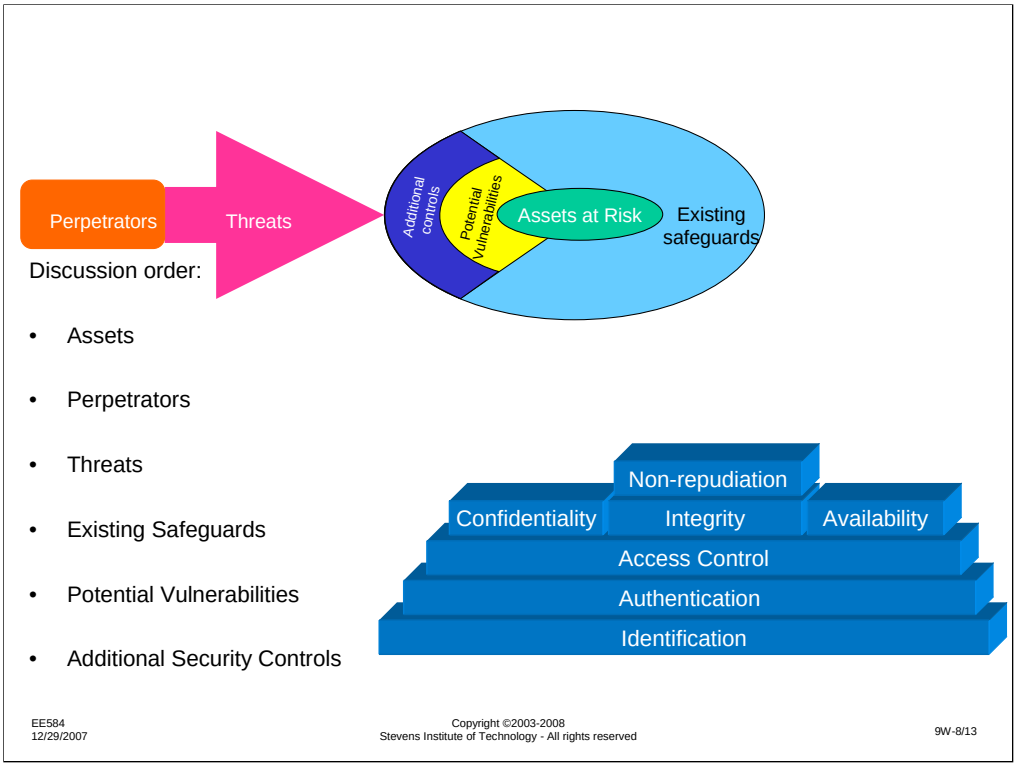
Threats: What mischief can you get into? How would you do it?

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.

Assets

- ***Equipment***
  - ***Infrastructure***
  - ***Towers***
  - ***Radios***
  - ***Data network connections***
  - ***Wiring/fiber***
- ***Bandwidth***
- ***Spectrum***
- Information content – upload/download
- End terminals
  - Hardware
  - Software
  - Operating system
- ***Servers***
  - ***Hardware***
  - ***Software***
  - ***Operating system***
- ***Routers/bridges***
- Protocols
- Privacy of users
- Accuracy of information
- End users
  - Privacy
  - Identity
  - Usage
- Routing tables

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

Hackers
Terrorists
Nature
Spoofers
Amateur radio operators
Network operators
Users
Equipment competitors
Network competitors
Resellers
Government (TIA, Patriot Act)
Community (change physical environment, deployment rules)

Threats

Destruction of communications facilities due to natural disaster (fire, earthquake, severe weather)
Monitor channel and obtain information to exploit
Jamming
Intentional overload of channel
- At RF
- At IP

Use the service to disseminate virus or other things to disrupt system
Misconfiguration of
- User terminal
- Service
- Network

Obtain a user's ID and authentication, masquerade as user
- Accessing their information
- Costing them usage

Misconfigure a router to send excess traffic over wireless link
Untraceability of wireless source allows bogus messages
Use latency of channel to make possible "insider" trading
Device cloning to avoid service charges

Existing Safeguards

Encryption of data
Firewalls/proxy server/NAT
Identification of users
SIM card (GSM/EDGE)
Access control lists
PIN/EID
Backup servers/routers
Diversity of service (multiple base stations)
Performance monitoring systems
Ability to reroute traffic
Expertise of network designers

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

Vulnerabilities

Multiple points of attack
- RF
- Terminal
- Server
- Network

Lack of mutual authentication (server to terminal)
Standardized/publicly known algorithms, protocols, crypto, etc.
Widely interconnected systems
User naivety
Channel latency
Little of no tamper protection
Inability to “black list” devices
Connectivity to Internet/public networks
Limited duration of backup power at basestations
Focus of failure could be mobile or could spread
No blocking during overload
Failures could lead to failures spreading thru network (lack of containment procedures)