Wireless Systems Security

EE/NiS/TM-584-A/WS

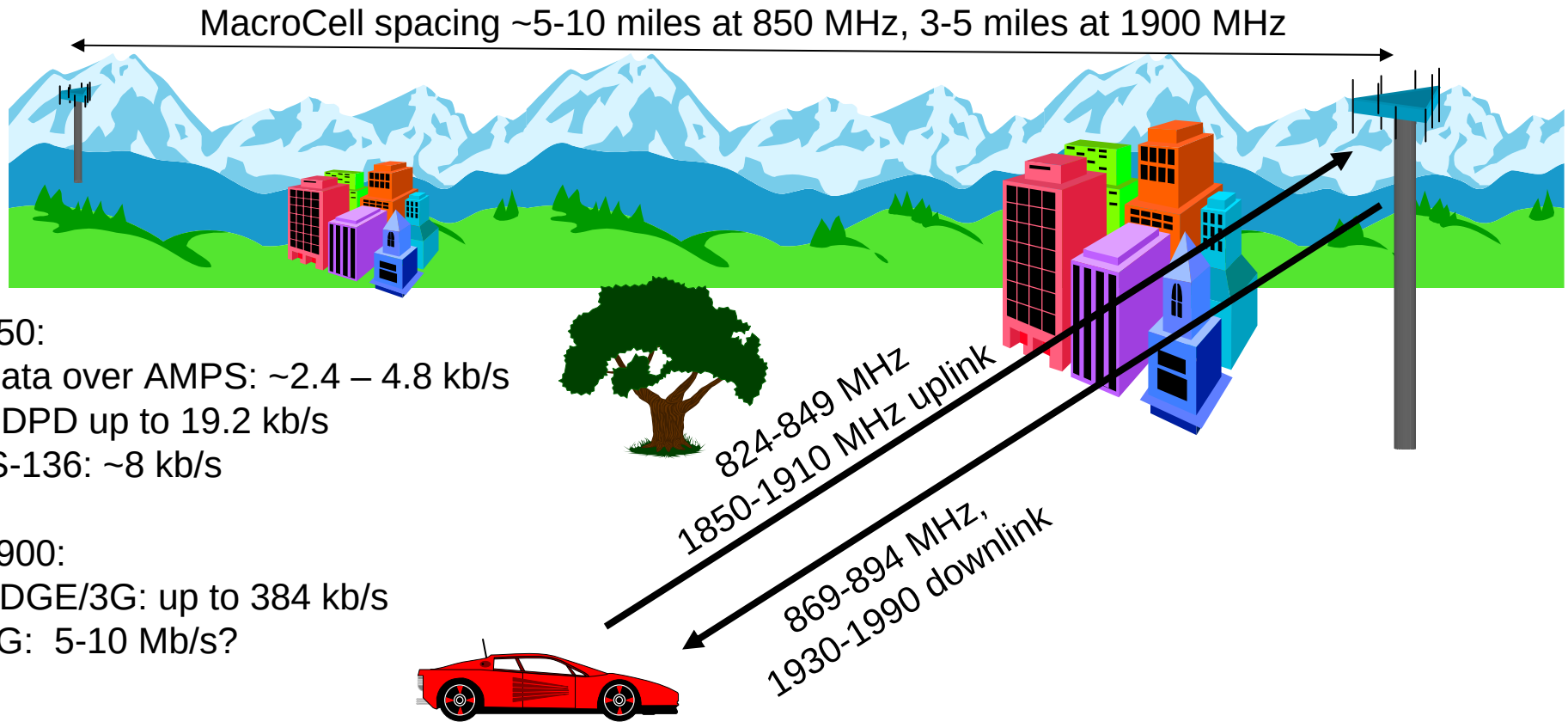
Bruce McNair
bmcnair@stevens.edu

Week 9

Case Study 5

Summary and observations

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

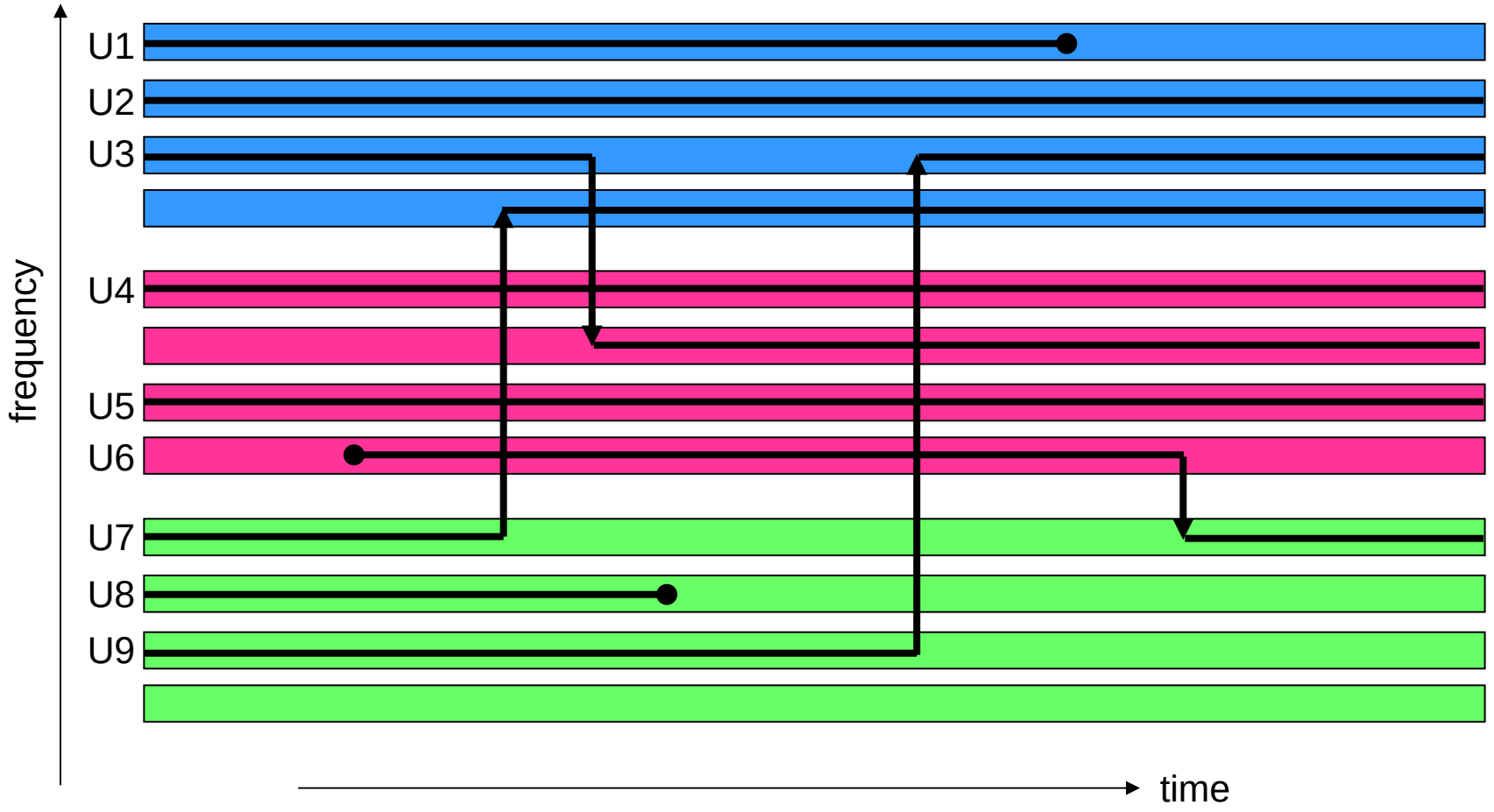


850:
Data over AMPS: ~2.4 – 4.8 kb/s
CDPD up to 19.2 kb/s
IS-136: ~8 kb/s

1900:
EDGE/3G: up to 384 kb/s
4G: 5-10 Mb/s?

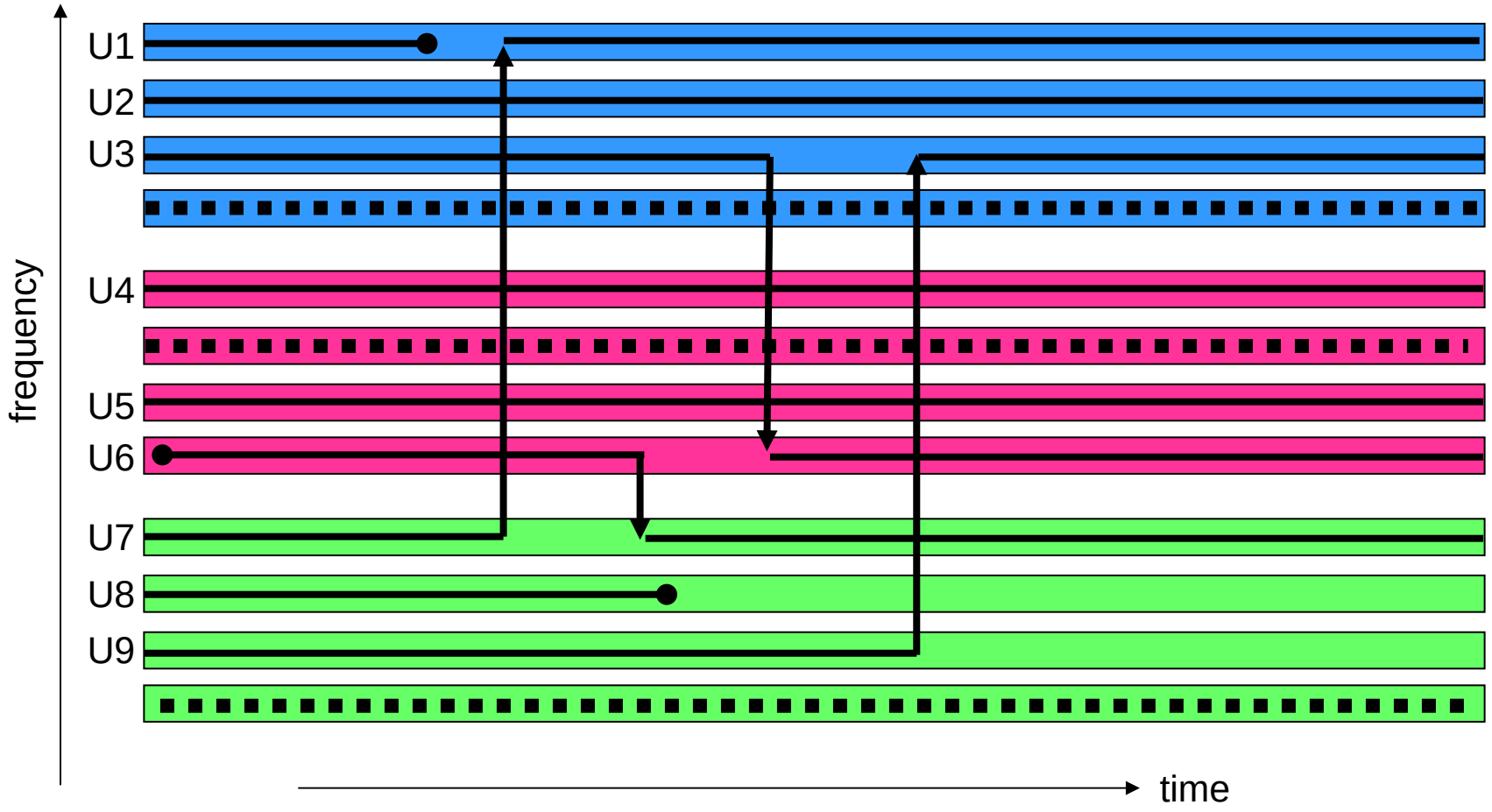
Cellular Data Systems: The Beginning: CDPD

- Consider three basestations, each with 4 frequencies available



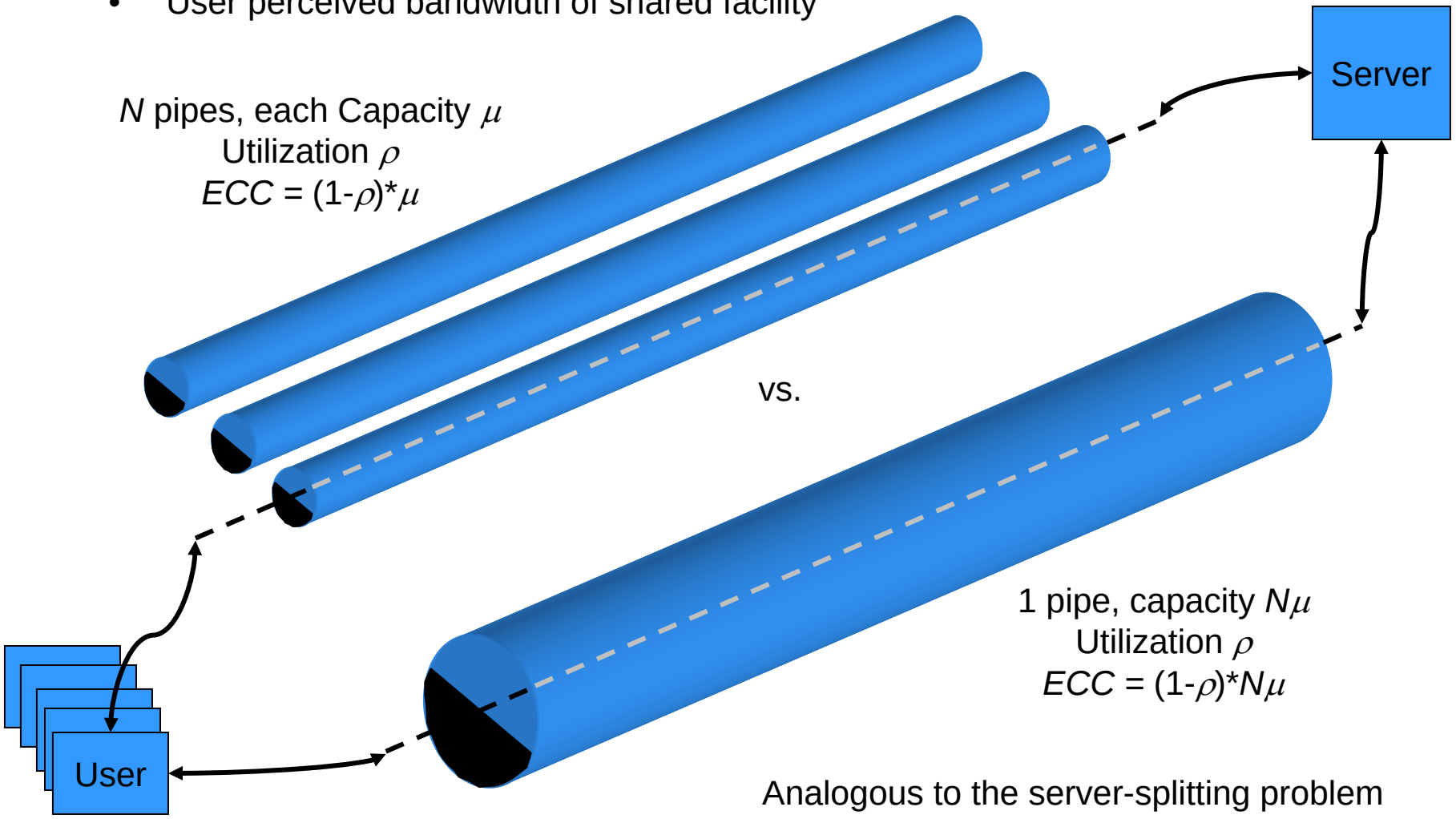
Cellular Data Systems:
CDPD as a service in it's own right

- Dedicate channels to CDPD operation



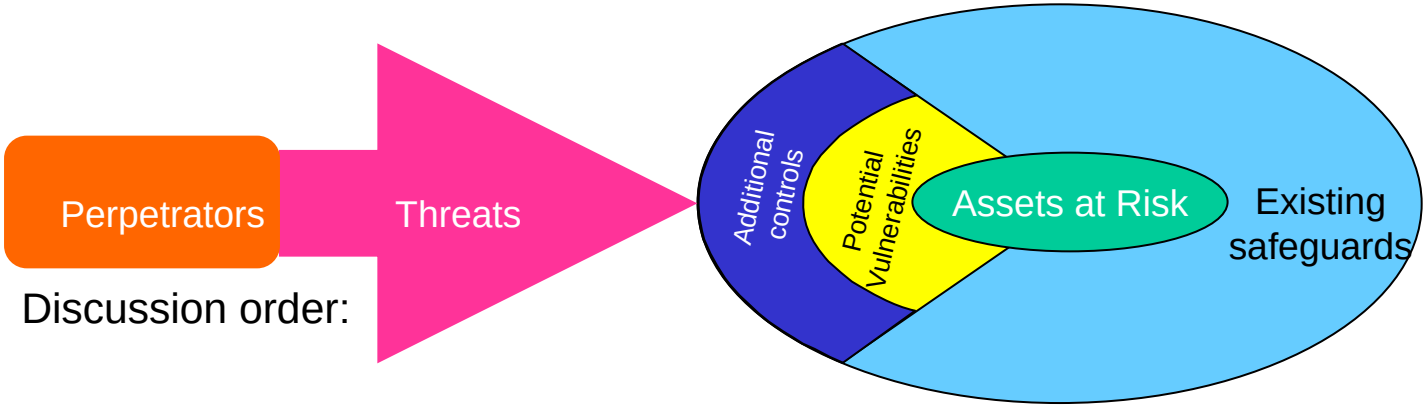
The Need for Higher Bandwidth Data Services

- User perceived bandwidth of shared facility



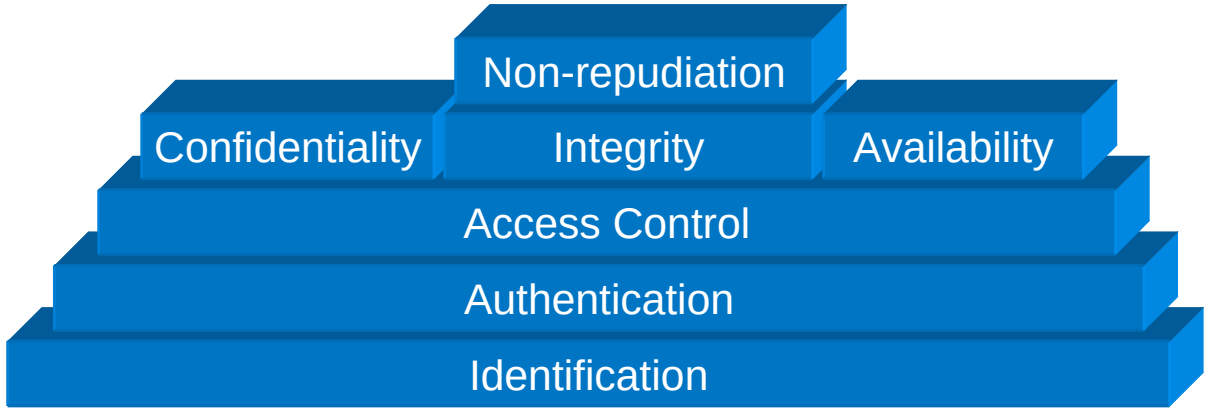
Analogous to the server-splitting problem

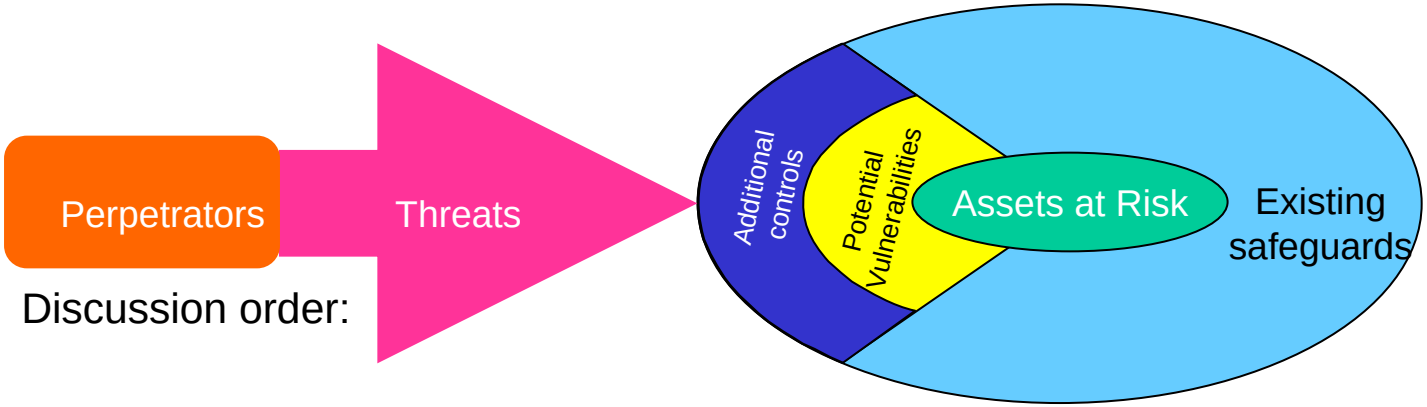
User perceived Equivalent Circuit Capacity



Discussion order:

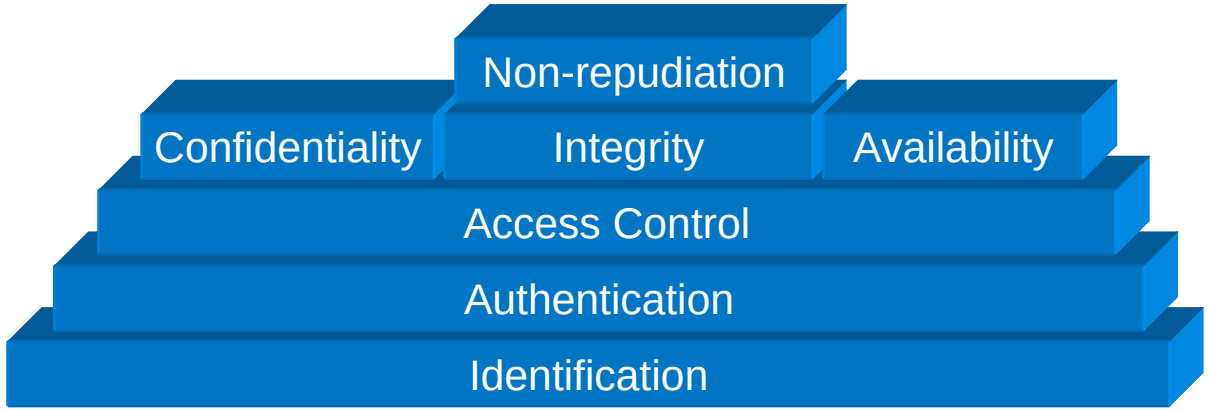
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls





Discussion order:

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



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

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

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)