Computer/Network Security

Agenda

- Security Overview
- Seven Key Concepts
- Wireless Fundamentals
- Certification
- Job Opportunity

Security is Business

Physical Security

Technological Security

Policies and Procedures

Security Concepts

- Authentication
- Authorization
- Confidentiality
- Data/Message Integrity
- Accountability
- Availability
- Non-Repudiation

Spear Phishing Attacks

Wireless

Difference between Wired and Wireless

- Wired:
  - Dedicated
  - CSMA/CD (Career Sense Multiple Access/Collision Detection)
- Wireless:
  - Not dedicated
  - Competition for usage
  - CSMA/CA (Career Sense Multiple Access/Collision Avoidance)
  - Susceptible to RF factors

Basic Concepts

2.4 GHz vs 5 GHz

[illegible]

Interference

Certification

- Vendor Specific:
  - CCNA
  - CCNA Security
  - Firewall:
    - Check Point (CCSA, CCSE)
    - Palo Alto (ACE, PCNSE)
- Vendor Neutral:
  - CompTIA A+/Network+/Security+
  - CWNP: Certified Wireless Network professional
  - CEH: Certified Ethical Hacker
  - CISSP: Certified Information Systems Security Professional
- Free Resource
  - MOOC: Massive Online Open Courses

Job Opportunity

Conclusion

- Turtle Shell Architecture
- Logs don's lie
- Security is like a fence around your house
- Social Engineering
  - Kevin Mitnick: Read his books
- It is a business:
  - Bad guys have an advantage.
  - Make yourself an expensive target
- Key Concepts:
  - AAA: Authentication, Authorization, Accounting
  - CIA: Confidentiality, Integrity, Availability

Computer/Network Security

Agenda

- Security Overview
- Seven Key Concepts
- Wireless Fundamentals
- Certification
- Job Opportunity

Security in Depth

Physical Security

Technological Security

Policies and Procedures

Security Concepts

- Authentication
- Authorization
- Confidentiality
- Data/Message Integrity
- Accountability
- Availability
- Non-Repudiation

Spear Phishing Attacks

Wireless

Difference between Wired and Wireless

- Wired:
  - Dedicated
  - CSMA/CD (Career Sense Multiple Access/Collision Detection)
- Wireless:
  - Not dedicated
  - Competition for usage
  - CSMA/CA (Career Sense Multiple Access/Collision Avoidance)
  - Susceptible to RF factors

Basic Concepts

2.4 GHz vs 5 GHz

Rogue

Interference

Certification

- Vendor Specific:
  - CCNA
  - CCNA Security
  - Firewall:
    - Check Point (CCSA, CCSE)
    - Palo Alto (ACE, PCNSE)
- Vendor Neutral:
  - CompTIA A+/Network+/Security+
  - CWNP: Certified Wireless Network professional
  - CEH: Certified Ethical Hacker
  - CISSP: Certified Information Systems Security Professional
- Free Resource
  - MOOC: Massive Online Open Courses

Job Opportunity

Conclusion

- Turtle Shell Architecture
- Logs don't lie
- Security is like a fence around your house
- Social Engineering
  - Kevin Mitnick: Read his books
- It is a business:
  - Bad guys have an advantage.
  - Make yourself an expensive target
- Key Concepts:
  - AAA: Authentication, Authorization, Accounting
  - CIA: Confidentiality, Integrity, Availability

Agenda

- Security Overview
- Seven Key Concepts
- Wireless Fundamentals
- Certification
- Job Opportunity

Security Is Holistic

- Physical Security
- Technological Security (related to software):
    - Application Security
    - Operating System Security
    - Network Security
- Policy and Procedure

Physical Security

- Protecting against information leakage - Document Theft
- Limited access to authorized locations and equipment
- Example: Dumpster Diving, Theft of equipment etc.

Technological Security

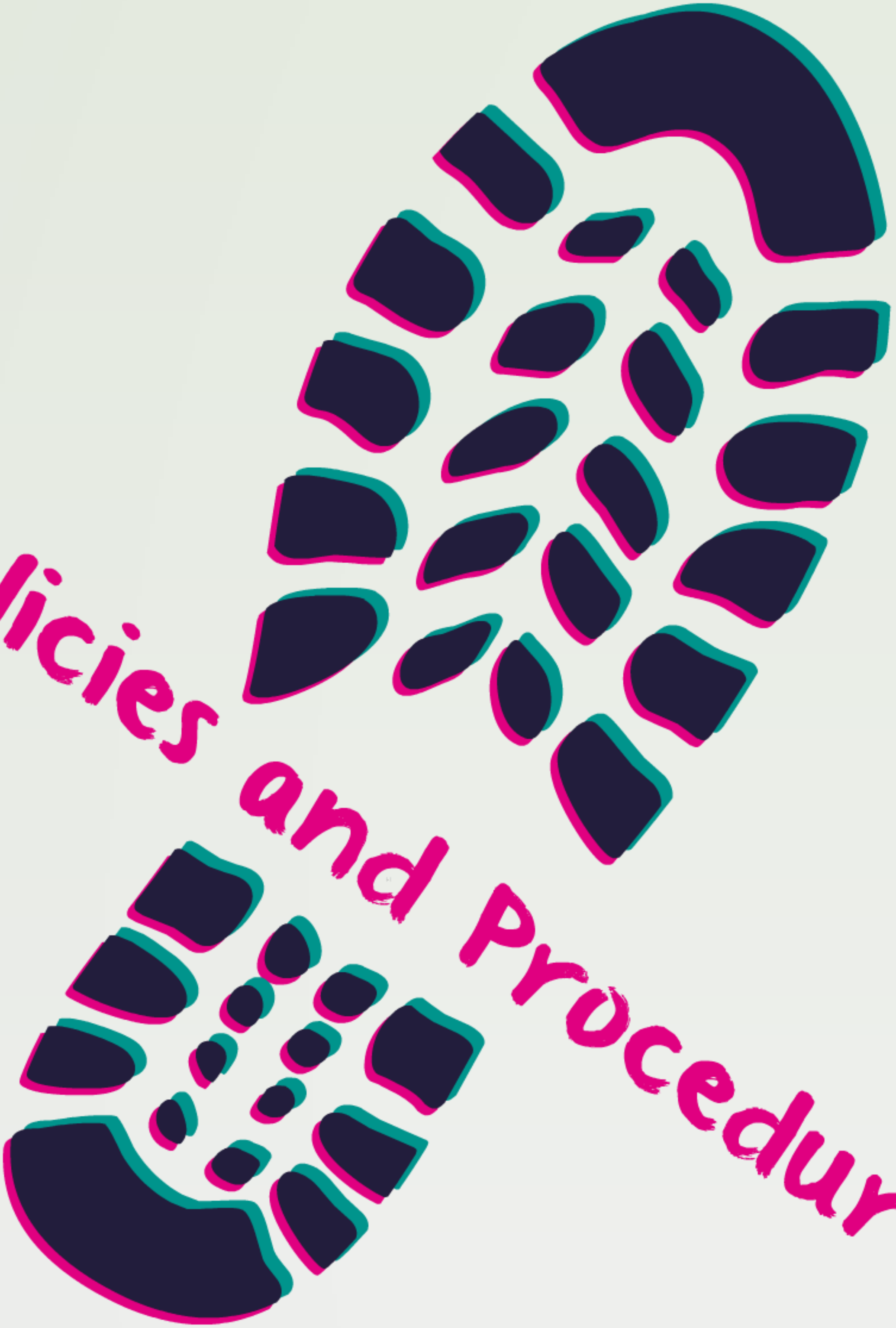
Application Security

- Strong identity verification:
  - Know who the user is
  - Log/Audit user access
- Configure application correctly:
  - Patch application
  - Change default admin passwords
- Server/Application/Data robustness
  - Outage can cause a lot of damage
  - Eg: DoS or DDoS

OS and Network Security

- Server Parches: Windows updates
- Network Security:
  - Miscellaneous traffic
  - BOT infections
- Tools useful:
  - Firewall
  - IPS/IDS
  - Antivirus applications
  - Reliable logging: (logging are like your footsteps in sand)

Policies and Procedures



- Social Engineering attacks:
    - Phishing Emails
    - Phone calls
    - Misrepresenting ones identity
- Safeguard sensitive corporate data
- Educate employees:
    - REMEMBER: Majority of attacks are initiated from within

Security Concepts

- Authentication
- Authorization
- Confidentiality
- Data/Message Integrity
- Accountability
- Availability
- Non-Repudiation

Common Security Characters

• Alice and Bob:	Good Guys
• Eve:	Passive Eavesdropper
• Mallory:	Active Eavesdropper
• Trent:	Trusted by Alice and Bob

Authentication

- Identity Verification: How can you be sure Bob is talking to Alice
  - Something you **know** (Password: OTP)
  - Something you **have** (SecureID cards, ATM cards)
  - Something you **are** (Biometrics)
- ***REMEMBER***:
  - Strength of authentication depends on difficulty of forging/cracking.
  - Add complexity: Two factor authentication
    - ATM cards
    - Fingerprint + PIN

Authorization

- Who you are vs What access you have
  - Is Alice allowed to access a certain document
  - Can user perform a certain action
- Restrict Access
  - ACL: Access control List
  - Role Based Access

Home Work: What is Bell LaPadula Model?

Confidentiality

- Goal: Keep the contents of communication to be a secret
- Eve (eavesdropper) should not be able to retrieve the data
- Can be achieved:
  - Encryption
  - Cryptography

Data/Message Integrity

- Goal: Mallory (Active Eavesdropper) cannot tamper with the communication between Alice and Bob
- Data Integrity = No Corruption

Techniques:

- Hashing: MD5, SHA-1
- Checksums (CRC)

Accountability

- Goal: Who conducted the action
- Requirements:
  - Logging and Audit trails
  - Secure Time-stamp
  - Data Integrity: Cannot modify

Remember: If the requirements are not fulfilled the attacker can successfully hide there tracks.

Availability

- Goal: Achieve close to 100% uptime
- Add redundancy
- Legitimate / authorized use

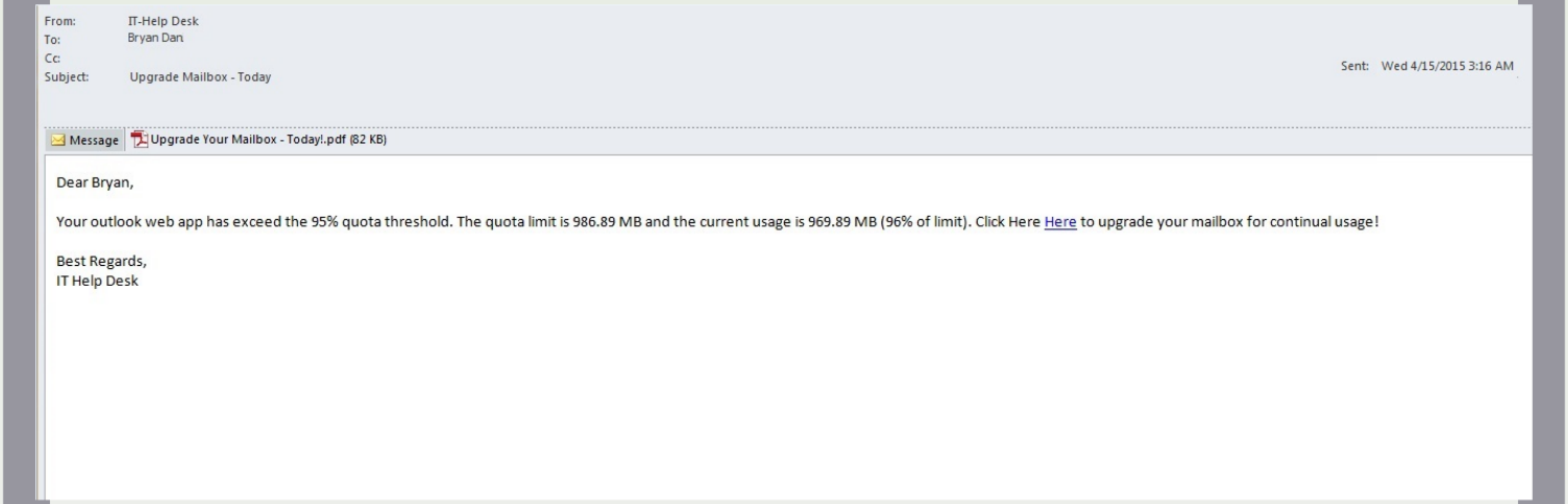
Remember:

- This is a collaborative effort
- Goal of DoS and DDoS is to reduce availability

Non-Repudiation

- Goal: Undeniability of a transaction
- Generate Evidence
- Digital Signature

Spear Phishing Attacks



From: IT-Help Desk
To: Bryan Dan
Cc:
Subject: Upgrade Mailbox - Today

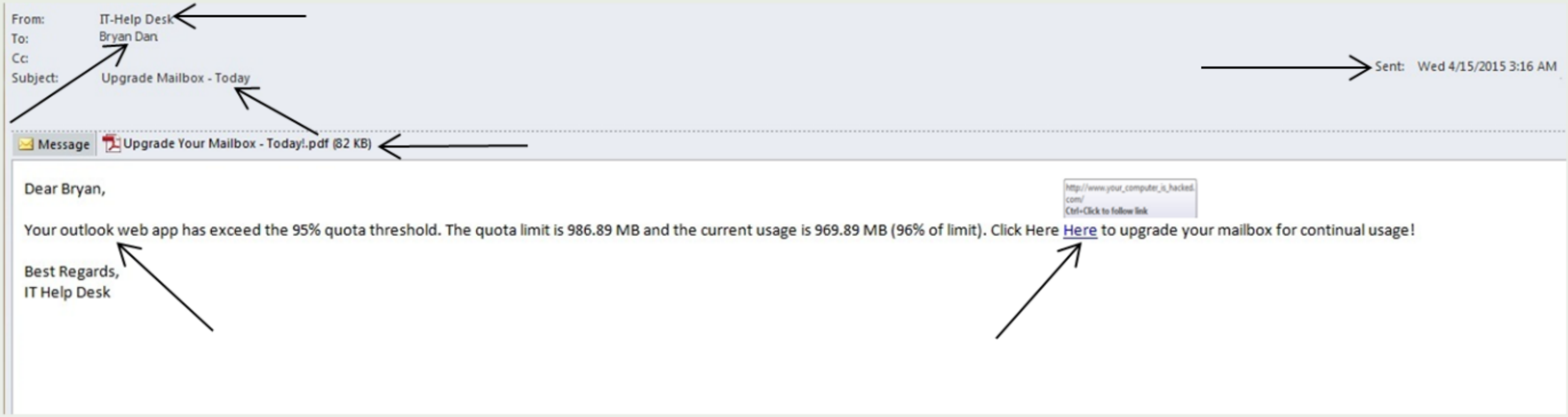
Sent: Wed 4/15/2015 3:16 AM

Upgrade Your Mailbox - Today!.pdf (82 KB)

Dear Bryan,

Your outlook web app has exceed the 95% quota threshold. The quota limit is 986.89 MB and the current usage is 969.89 MB (96% of limit). Click Here Here to upgrade your mailbox for continual usage!

Best Regards,
IT Help Desk



From: IT-Help Desk
To: Bryan Dan
Cc:
Subject: Upgrade Mailbox - Today

Sent: Wed 4/15/2015 3:16 AM

Upgrade Your Mailbox - Today!.pdf (82 KB)

Dear Bryan,

http://www.your_computer_is_hacked.com/
Ctrl+Click to follow link

Your outlook web app has exceed the 95% quota threshold. The quota limit is 986.89 MB and the current usage is 969.89 MB (96% of limit). Click Here Here to upgrade your mailbox for continual usage!

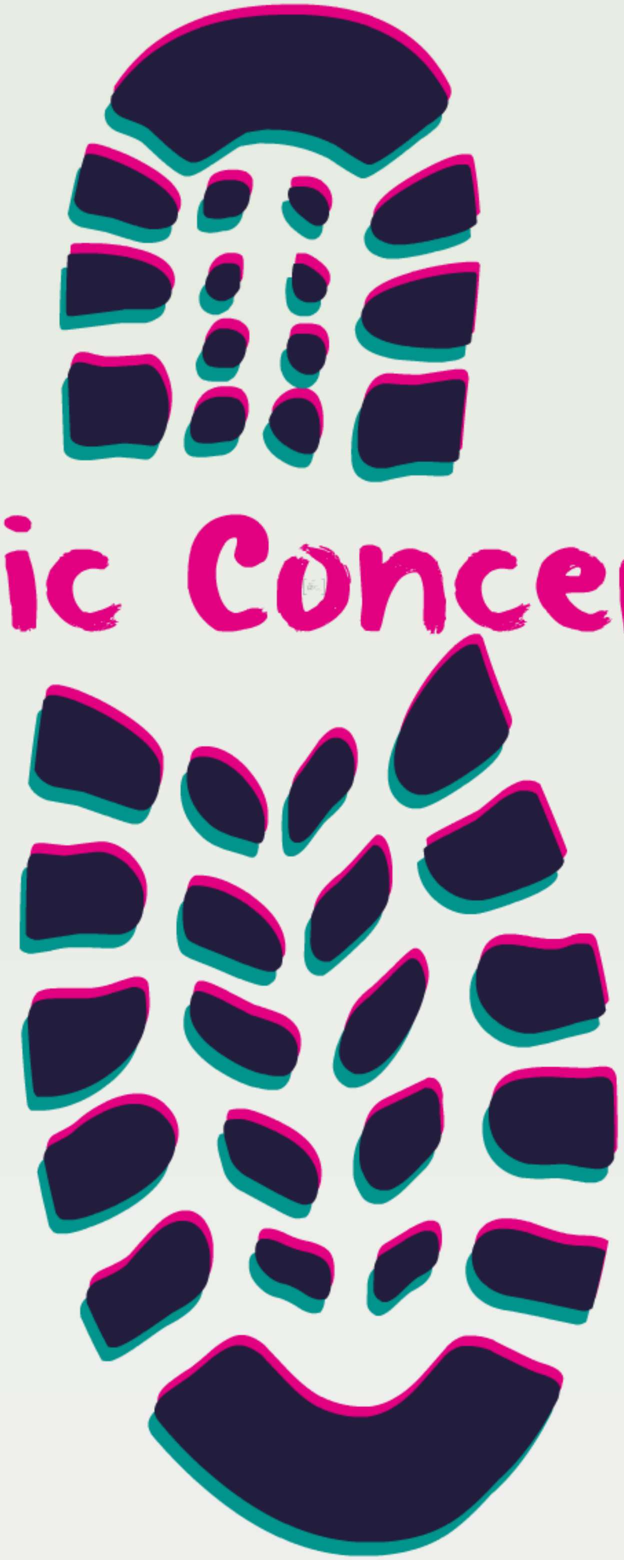
Best Regards,
IT Help Desk

Wireless

Difference between Wired and Wireless

- Wired:
  - Dedicated
  - CSMA/CD (Career Sense Multiple Access/Collision Detection)
- Wireless:
  - Not dedicated
  - Competition for usage
  - CSMA/CA (Career Sense Multiple Access/Collision Avoidance)
  - Susceptible to RF factors

Basic Concepts



Remember

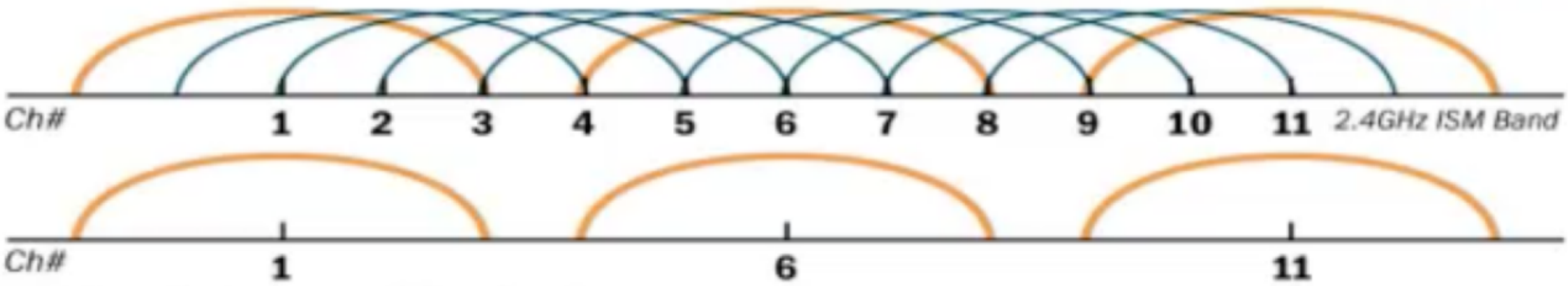
- Range/Coverage/Capacity
  - Range and Coverage are for taken granted
  - Plan for Capacity
- More susceptible to RF factors:
  - Noise: Noise is unwanted electrical or electromagnetic energy
  - Interference: Signal is distorted
  - Attenuation: Signal passes through material
- 2.4GHz vs 5 GHz
- Clients are competing (not dedicated connection)
- Connection will be as fast as the slowest connection

2.4 GHz vs 5 GHz

802.11A/B/G/N: CHANNEL BREAKDOWN

802.11b/g/n

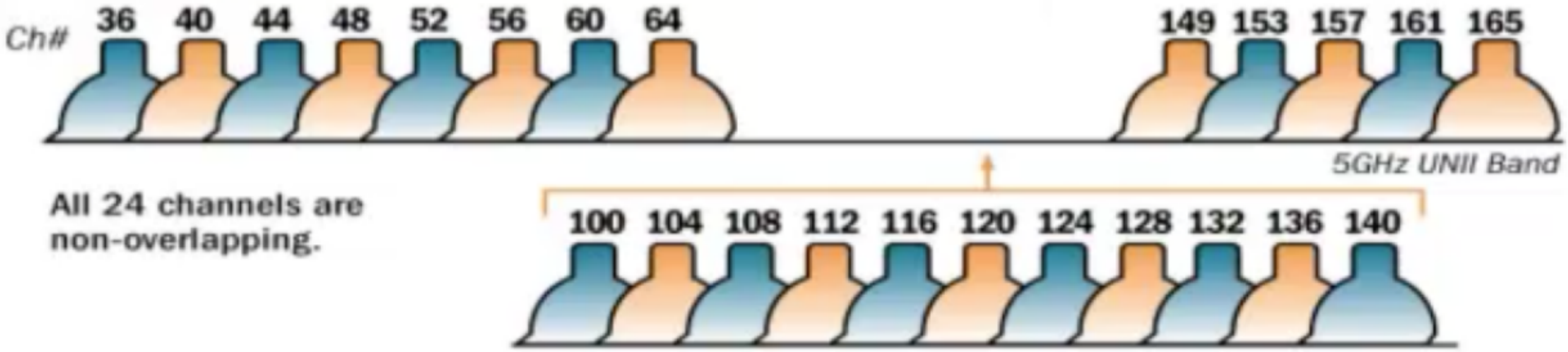
11 channels are available in the U.S. for 802.11b/g/n



Only 3 channels are non-overlapping.

802.11a/n

24 channels are available in the U.S. for 802.11a/n



All 24 channels are non-overlapping.

Note: The above graphic identifies North American channel assignments, channels varies for different countries based on their regulatory domains

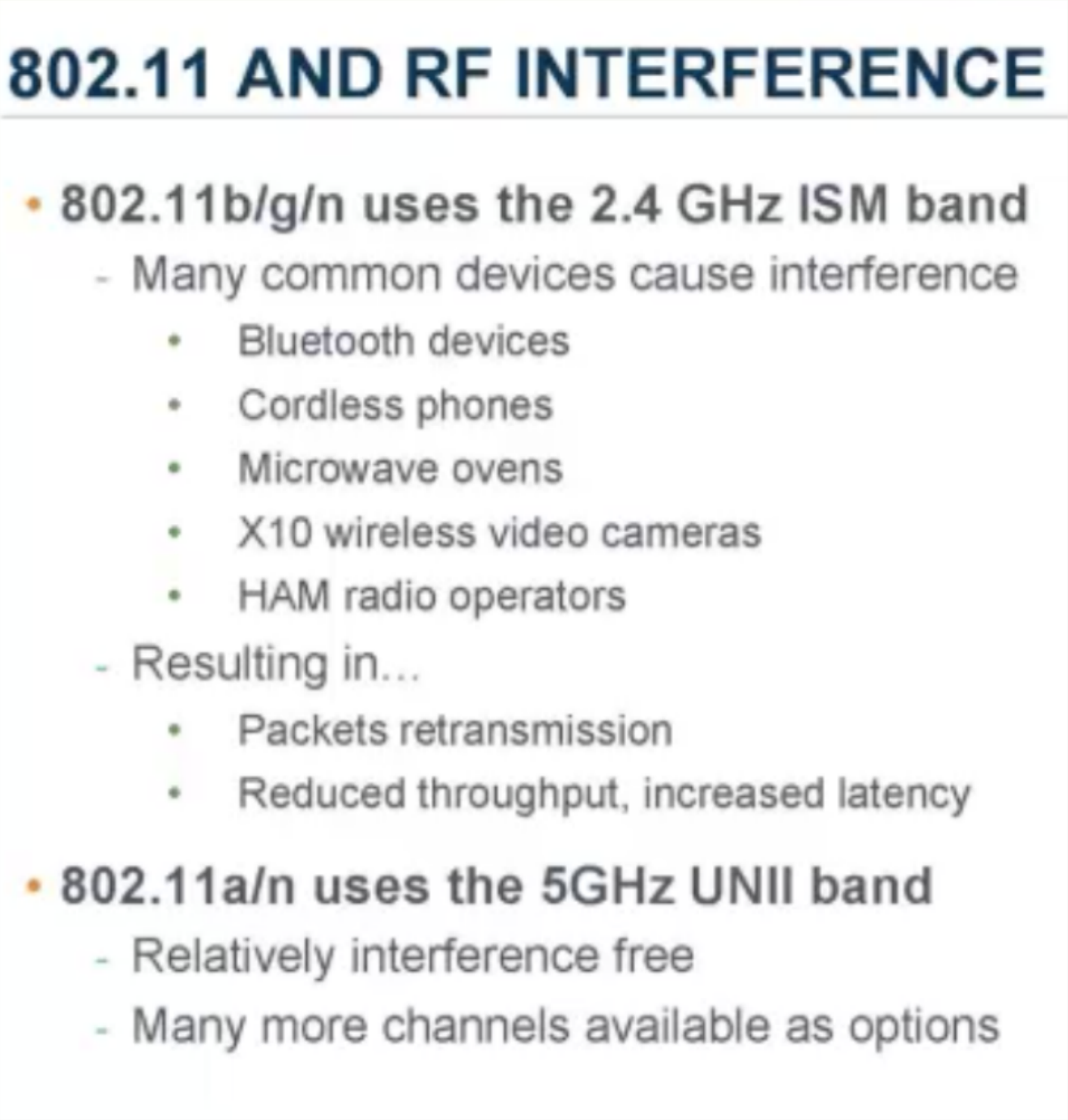
BANDS, CHANNELS AND CAPACITY

Two frequency bands used in Wi-Fi (27* channels)

- **2.4GHz – used by 802.11b/g/n clients**
  - **3** non-overlapping channels (differs by geo region)
  - Limited bandwidth, prone to interference
- **5GHz – used by 802.11a/n clients**
  - **Up to 24** non-overlapping channels (differs by geo region)
  - 8X the bandwidth, Less potential for interference

2.4GHz
VS
5GHz

Interference

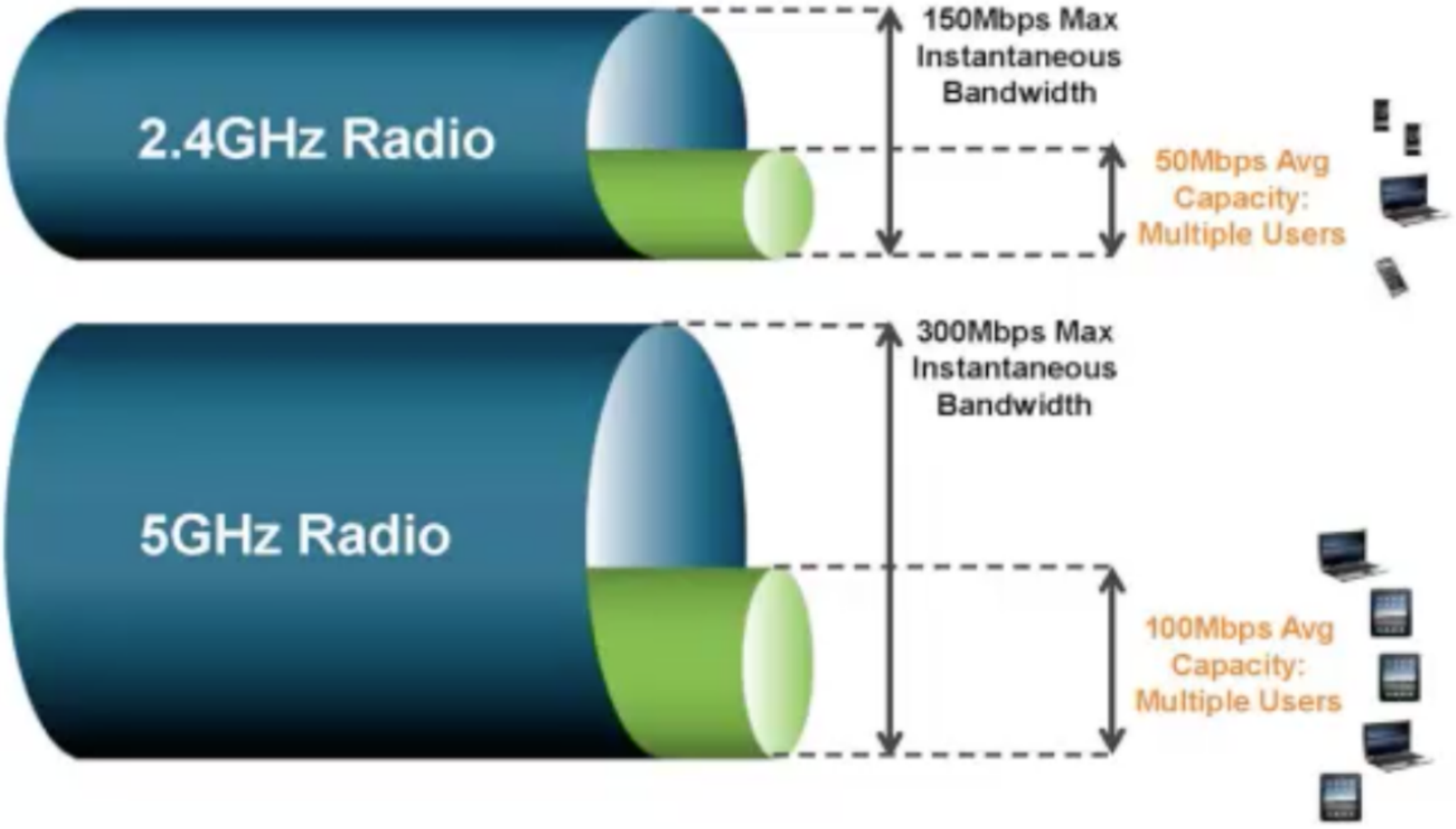


802.11 AND RF INTERFERENCE

- **802.11b/g/n uses the 2.4 GHz ISM band**
  - Many common devices cause interference
    - Bluetooth devices
    - Cordless phones
    - Microwave ovens
    - X10 wireless video cameras
    - HAM radio operators
  - Resulting in…
    - Packets retransmission
    - Reduced throughput, increased latency
- **802.11a/n uses the 5GHz UNII band**
  - Relatively interference free
  - Many more channels available as options

Radio

UNDERSTANDING RADIO CAPACITY (1)



2.4GHz Radio

150Mbps Max Instantaneous Bandwidth

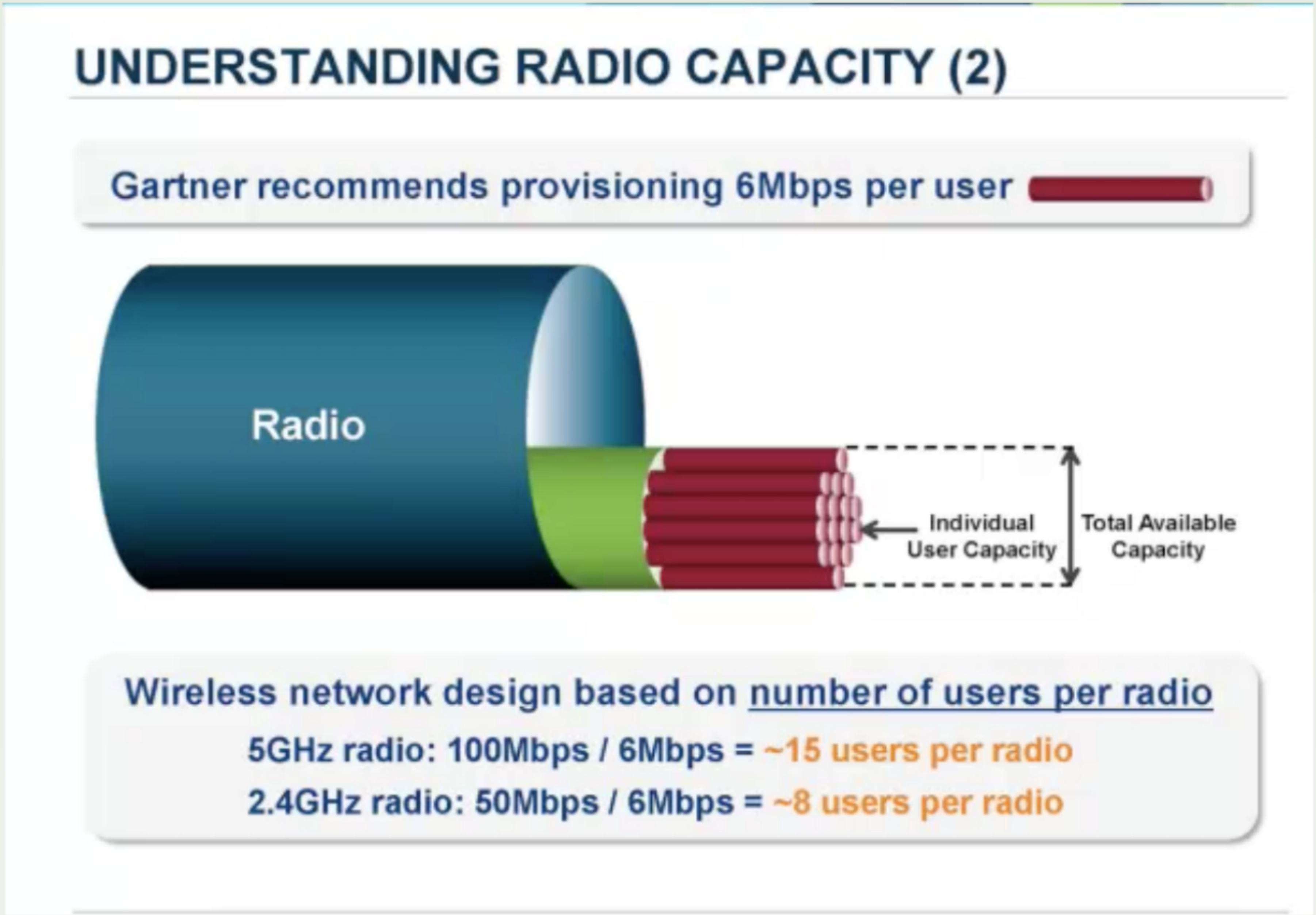
50Mbps Avg Capacity: Multiple Users

5GHz Radio

300Mbps Max Instantaneous Bandwidth

100Mbps Avg Capacity: Multiple Users

In a Wi-Fi network, radio capacity is reduced by protocol overhead and is shared by multiple users



UNDERSTANDING RADIO CAPACITY (2)

Gartner recommends provisioning 6Mbps per user

Wireless network design based on <u>number of users per radio</u>

5GHz radio: 100Mbps / 6Mbps = ~15 users per radio

2.4GHz radio: 50Mbps / 6Mbps = ~8 users per radio

Certification

- Vendor Specific:
  - CCNA
  - CCNA Security
  - Firewall:
    - Check Point (CCSA, CCSE)
    - Palo Alto (ACE, PCNSE)
- Vendor Neutral:
  - CompTIA A+/Network+/Security+
  - CWNP: Certified Wireless Network professional
  - CEH: Certified Ethical Hacker
  - CISSP: Certified Information Systems Security Professional
- Free Resource
  - MOOC: Massive Online Open Courses

Job Opportunity

Jobs

- Security Administrator / Engineer
- Network Security Administrators / Engineers
- Firewall Administrators / Engineers
- Desktop Security Administrators
- Enterprise Security Architects
- IT Security Officers
- Penetration Testers (White Hat Hackers)
- TAC Support: CISCO, Check Point, Palo Alto
- Consulting Jobs
- CISO: Chief Information Security Officer
- Network / Computer Security Professor

Conclusion

- Turtle Shell Architecture
- Logs don's lie
- Security is like a fence around your house
- Social Engineering
    - Kevin Mitnick: Read his books
- It is a business:
    - Bad guys have an advantage.
    - Make yourself an expensive target
- Key Concepts:
    - AAA: Authentication, Authorization, Accounting
    - CIA: Confidentiality, Integrity, Availability

Computer/Network Security

Agenda

- Security Overview
- Seven Key Concepts
- Wireless Fundamentals
- Certification
- Job Opportunity

Security in Depth

Physical Security

Technological Security

Policies and Procedures

Security Concepts

- Authentication
- Authorization
- Confidentiality
- Data/Message Integrity
- Accountability
- Availability
- Non-Repudiation

Spear Phishing Attacks

Wireless

Difference between Wired and Wireless
- Wired:
  - Dedicated
  - CSMA/CD (Career Sense Multiple Access/Collision Detection)
- Wireless:
  - Not dedicated
  - Competition for usage
  - CSMA/CA (Career Sense Multiple Access/Collision Avoidance)
  - Susceptible to RF factors

Basic Concepts

2.4 GHz vs 5 GHz

[illegible]

Interference

Certification

- Vendor Specific:
  - CCNA
  - CCNA Security
  - Firewall:
    - Check Point (CCSA, CCSE)
    - Palo Alto (ACE, PCNSE)
- Vendor Neutral:
  - CompTIA A+/Network+/Security+
  - CWNP: Certified Wireless Network professional
  - CEH: Certified Ethical Hacker
  - CISSP: Certified Information Systems Security Professional
- Free Resource
  - MOOC: Massive Online Open Courses

Job Opportunity

Conclusion

- Turtle Shell Architecture
- Logs don't lie
- Security is like a fence around your house
- Social Engineering
  - Kevin Mitnick: Read his books
- It is a business:
  - Bad guys have an advantage.
  - Make yourself an expensive target
- Key Concepts:
  - AAA: Authentication, Authorization, Accounting
  - CIA: Confidentiality, Integrity, Availability