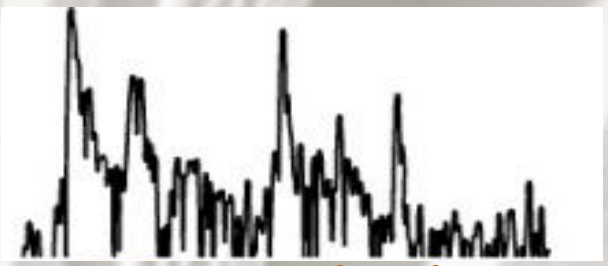


CYBER WARFARE IN THE WIRELESS WORLD

WHAT YOU DON'T KNOW *CAN* HURT YOU

LT D.A. Brown, CDR T.O. Walker, Ph.D., C. R. Anderson, Ph.D.
United States Naval Academy

Cyber Warfare in the Wireless World

- Overview
  - Overview of the Cyber Domain
  - Overview of the Cyber Wireless Component
  - Vulnerabilities and Exploits
  - Playing Defense
  - Case Studies
  - Open Research Questions
  - Conclusion / Questions

The opinions expressed herein are the views of the authors and do not necessarily reflect the views of the Navy, DoD, or United States Government.

What is the Cyber Domain?

Image from "The Matrix" © Warner Bros. Pictures

Current US DoD Definition:

"A global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

- **Key words to consider**
  - Global – cyber is something worldwide.
  - Domain – cyber is a "realm" or "territory".
  - (Big I) Internet – cyber is commercial/military, "wild west"/rules and laws, Protocols/Routing/Security.
  - Embedded – cyber exists even in "disconnected" systems.

Consider the "cyber world" in terms of a Domain

Consider world in terms of four domains:

Note **cross-domain interfaces** – transition from one domain to another:

- Sea – Land at a Port
- Air – Land at Airport

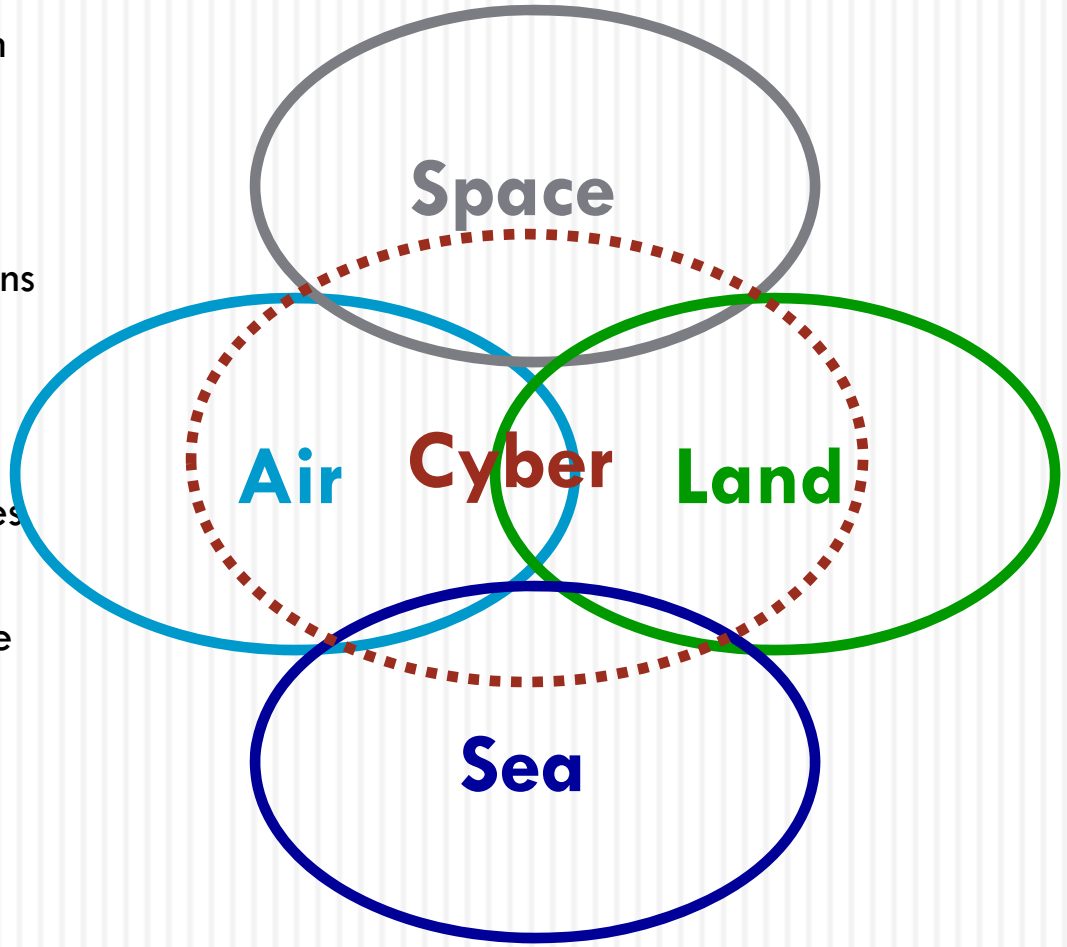
Events in one domain can impact what happens in other domains:

- Poor weather limit movement in Air, causing supply shortages in Land.

The **Cyber Domain** overlays and encompasses all four Physical Domains.

The Cyber Domain has many (if not all) of the same qualities as a physical domain:

- Domain Interfaces
- Laws/Regulations
- Structure and Order



What happens in the Cyber Domain can impact the Physical Domains!

The Cyber Domain pyramidal model

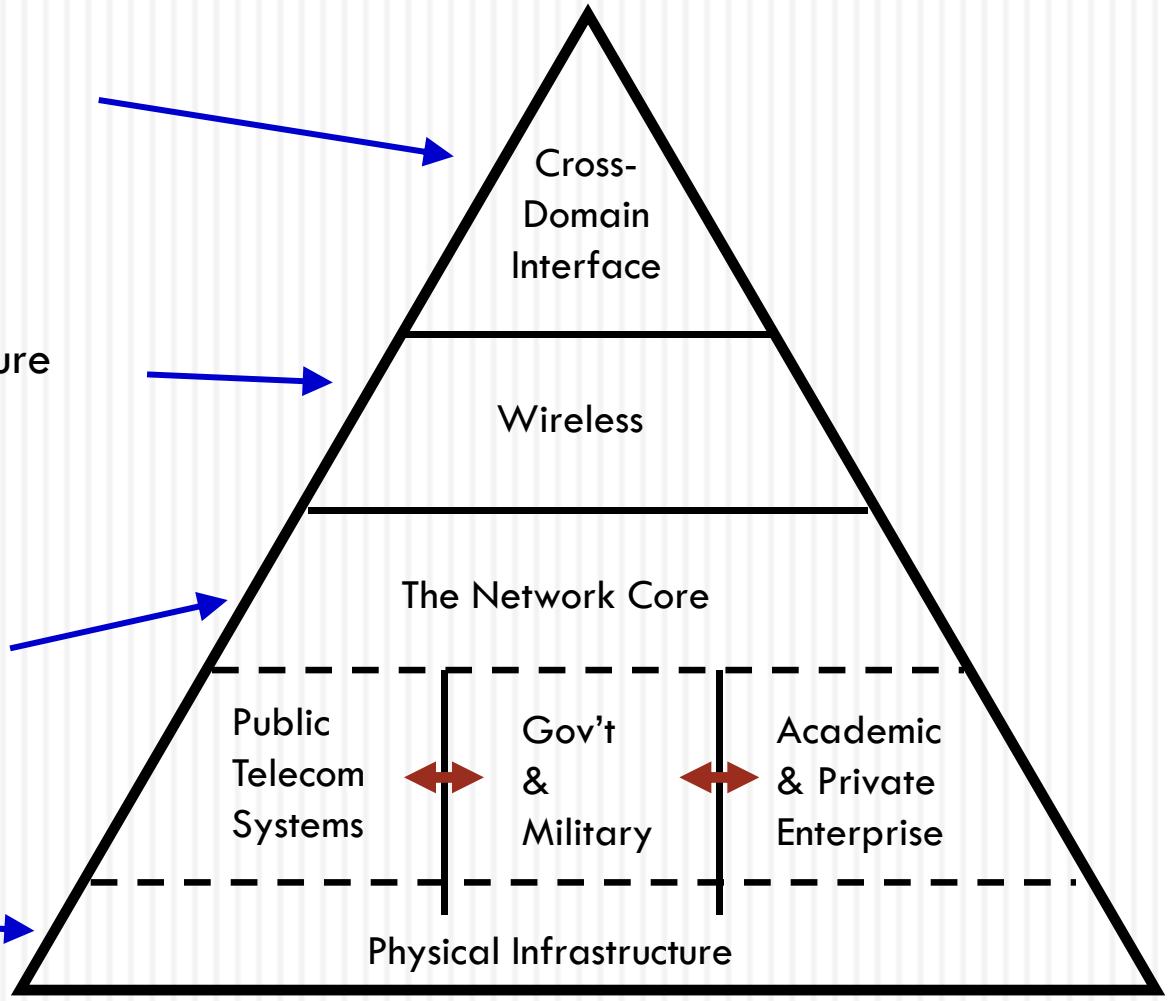
User Applications

↳ User Interface Device
e.g., smart phone,
PC, terminal.

Wireless standard and infrastructure
e.g., 802.11, CDMA2000, ZigBee

Network stack/protocol
Physical servers/routers
Physical/logical barriers
Physical/logical security
Inherent Trust in System!

Physical copper wire or
fiber cable.

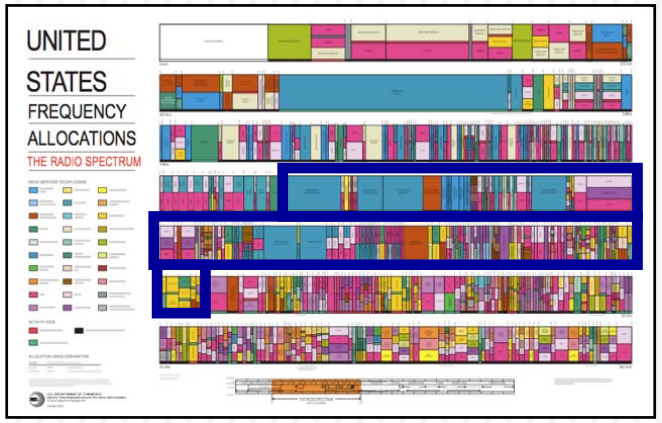


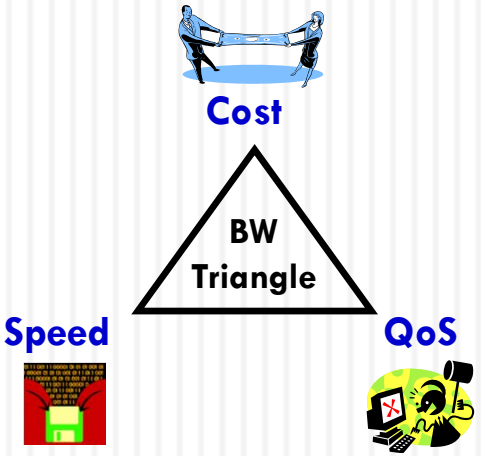
Why is wireless a critical component of the cybersecurity discussion?

Wireless has three key ingredients that complicate the discussion of cybersecurity/cyberwarfare:

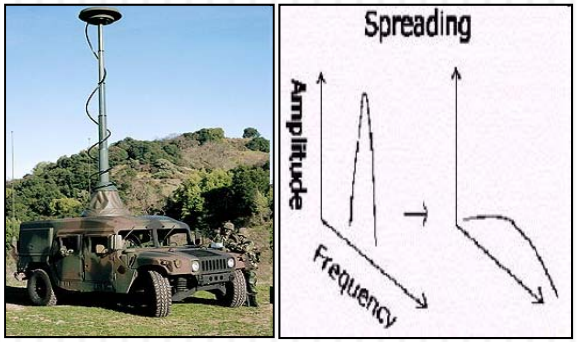
Spectrum – Availability and Location?
Bandwidth – How much, how expensive, how reliable?
Covertness – How well is your signal hidden?

"Good" Spectrum is severely limited



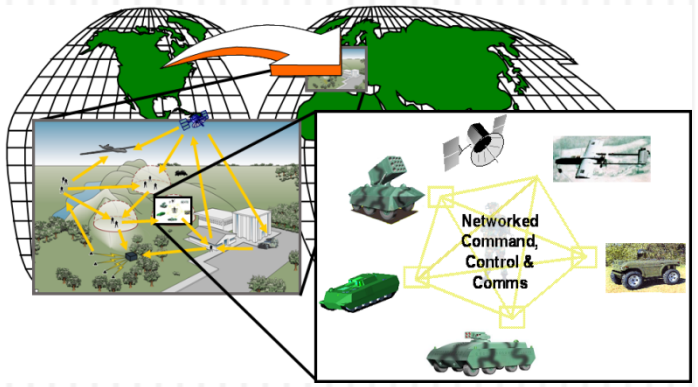


Wireless adds Physical and Spectrum security risks



The Wireless Key: How much of each do we need in order to close the link?

Cyberwarfare from a military perspective



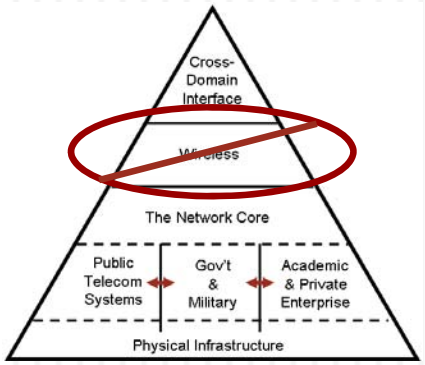
Military Comms/Cyber Goal:

Assured communications anywhere in the world with zero infrastructure and zero setup time.

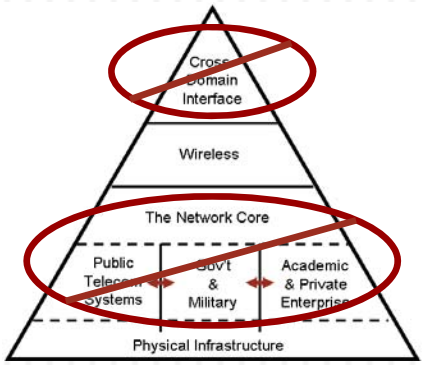
Assets that are hardened against cyberattacks and adapt to evolving attack vectors.

Cyberwarfare is a denial of the Cyber Domain.

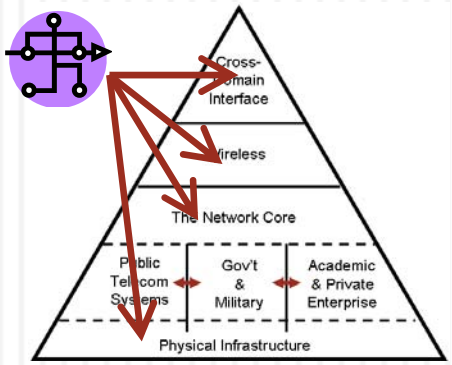
Denial of Spectrum



Denial of Computing

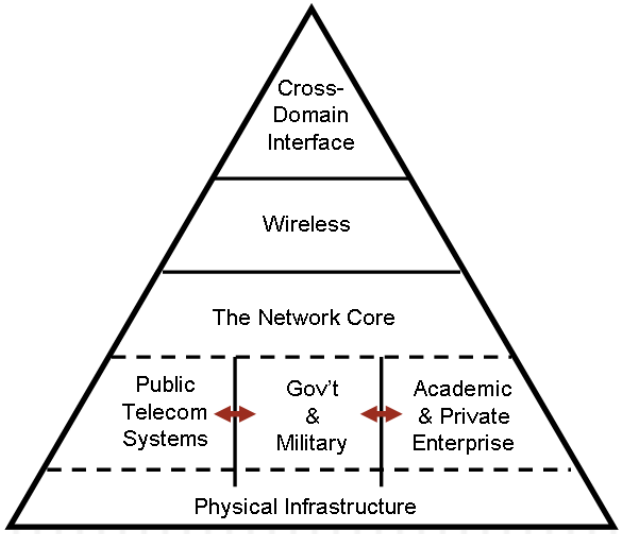


Attack Into Systems



Cyberwarfare will result in denial of a Physical Domain!

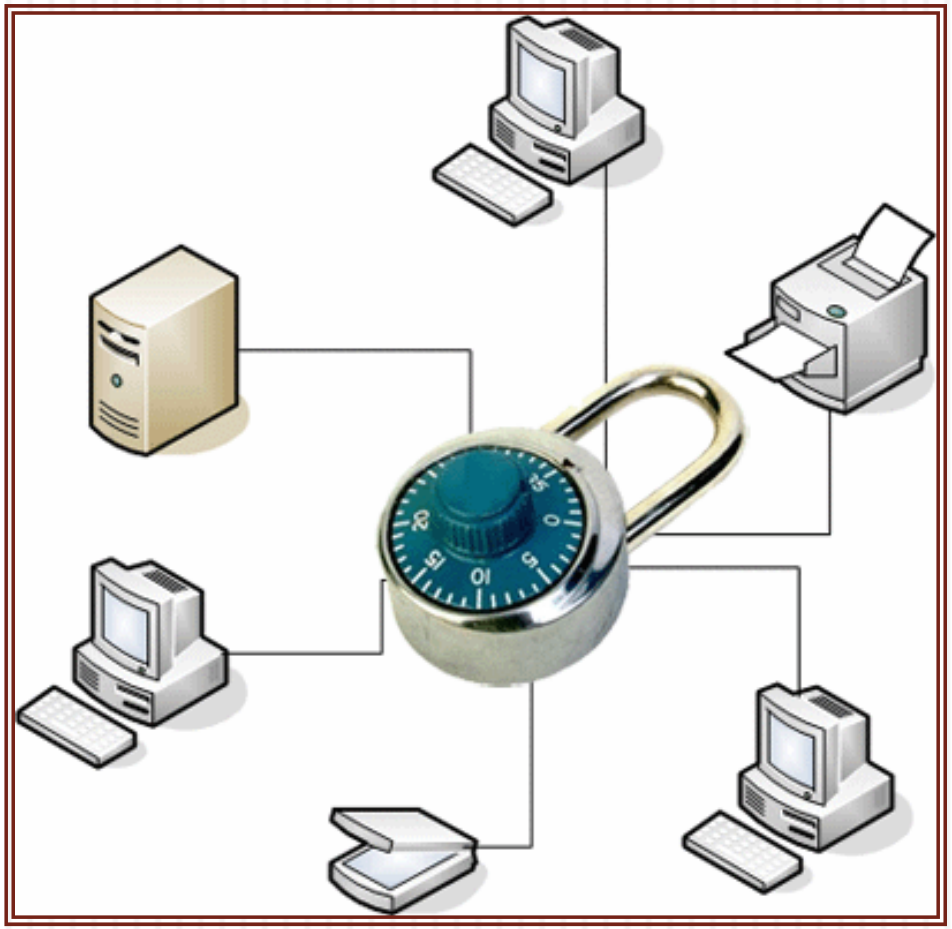
Tutorial organization and outline



- **Playing Offense**
  - Anatomy of a cyberattack
  - System Vulnerabilities
  - Wired vulnerabilities and exploits
  - Wireless vulnerabilities and exploits
- **The Cyber Battle**
- **Playing Defense**
  - Information Assurance
  - Best practices for security
  - Defense In Depth
- **Open Research Questions**

Vulnerabilities & Exploits

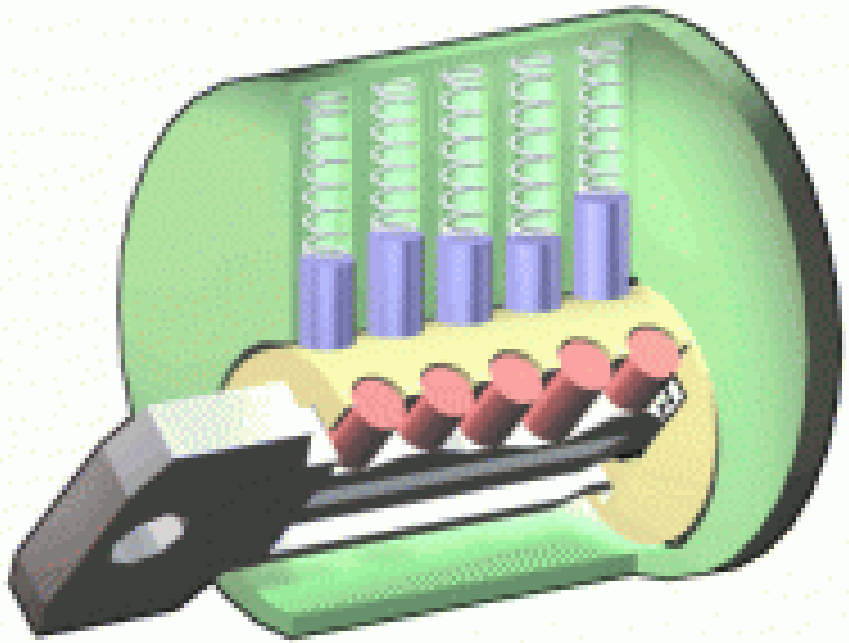
- Applicability
  - "Real Life" Analogy
- The Process
  - There *IS* a method to the madness
- Network Insecurity
  - System Level
  - Wired Networks
  - Wireless Networks



Come and knock on my door …

Intrusion Method	Exploited Vulnerability	Difficulty	Cost
Unlocked Door	Human	Easy	Free
Door Left Open	Human	Easy	Free
Stolen Key	Human	Medium	Free
Picked Lock	Lock	Medium	Low
Credit Card	Lock	Medium	Low
Drilled Lock	Lock	Medium	Medium
Crowbar	Door	Easy	Low
Hard Kick	Door	Easy	Free

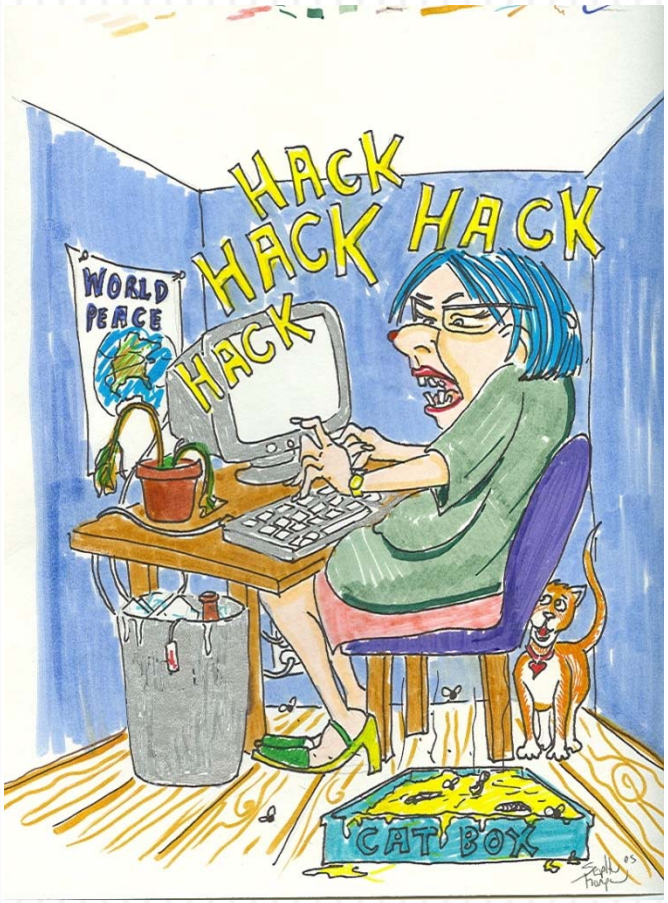
Minor Inconvenience



Anatomy Of An Attack

- 7 Basic Steps
  - Footprinting
  - Scanning
  - Enumerating
  - Gaining Access
  - Privilege Escalation
  - Covering Tracks
  - Creating a Backdoor

Who Can Do This?



- 3 Tiers of Hackers
  - Tier III : Script Kiddies
  - Tier II: IT Ninja
  - Tier I: 31337

How are we vulnerable?

- Information Assurance
- Cryptography
- Configuration (avoid defaults)
- Access Control

Information Assurance

- Confidentiality
  - Release of private data
  - Eavesdropping
- Integrity
  - Has anything changed?
- Availability
  - DOS
  - Deletion

Information Assurance

- Non-Repudiation
  - Trusted Sources
- Authentication
  - Authorized Access
  - Multi-Factor

Cryptography

- Symmetric
  - Fast
- Asymmetric
  - Public Key/ Private Key
  - Reusable: But be careful!
- Hashing
- Steganography
- File Level
- Disk Level
- Application Level

Tyranny of the Default

TRUST EVERYONE ☺

- User: admin
- Password: admin
- Encryption: WEP
- Pin: 0000
- HTTP
- Windows Firewall
- Server Defaults

Controlling Access

- Physical
  - MOST dangerous!
- Local User
  - Also dangerous!
  - Beware of Administrator
  - Strong Policies

- Remote User
  - Still bad!
  - Firewalls/VPNs

Controlling Access

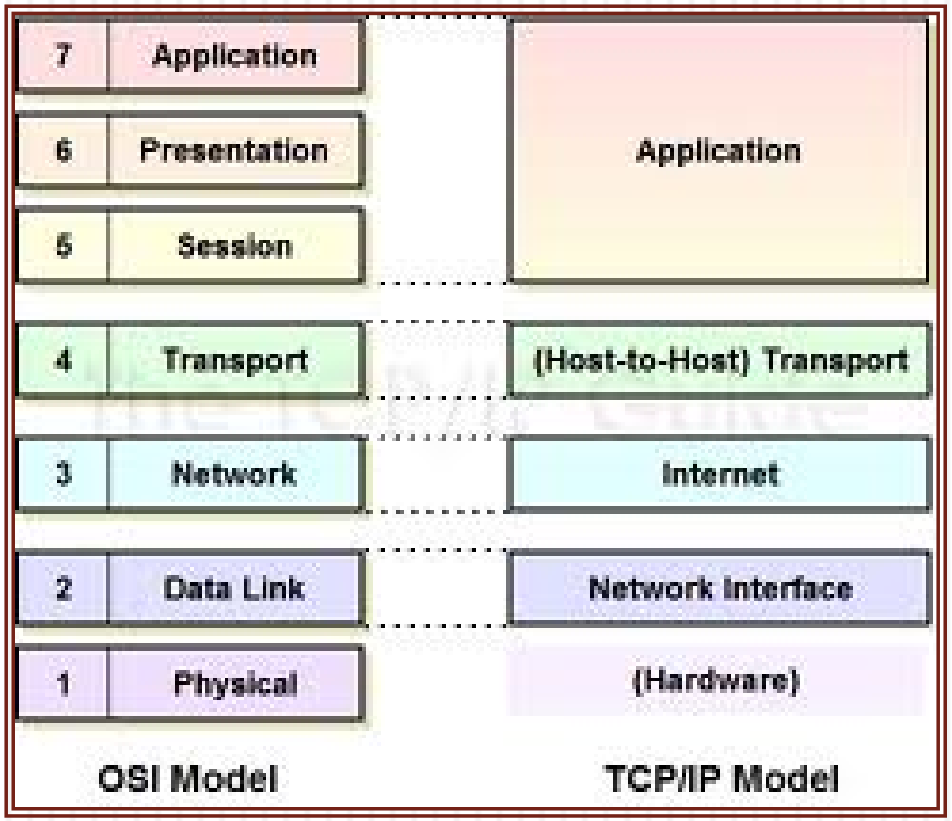
- USB Thumb Drives in DoD
- Freezing Memory
- Direct Access to Memory
  - Firewire
  - Thunderbolt
- Live Disks
  - Linux / System Recovery

Into the Ether

- IS THE NETWORK ARCHITECTURE FLAWED?

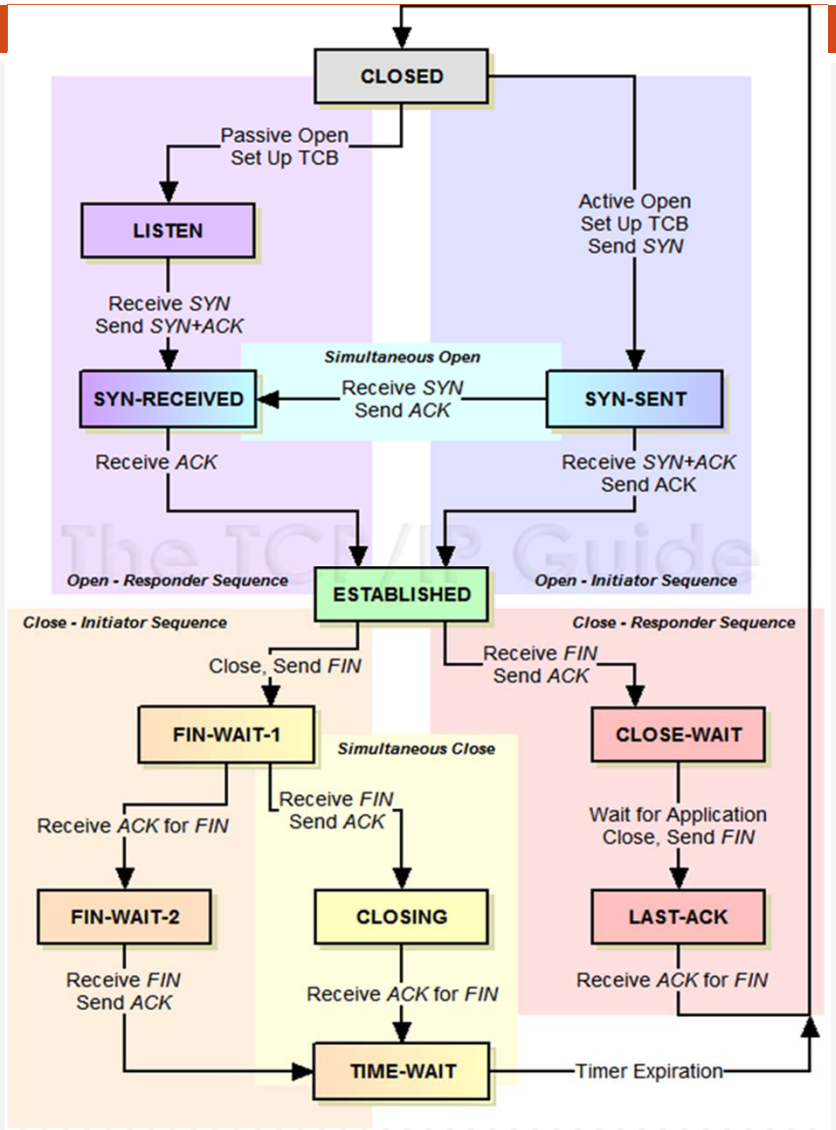
OSI Model Review

- 7 Layer Approach
  - How is a connection made between two systems on the internet to allow information exchange?



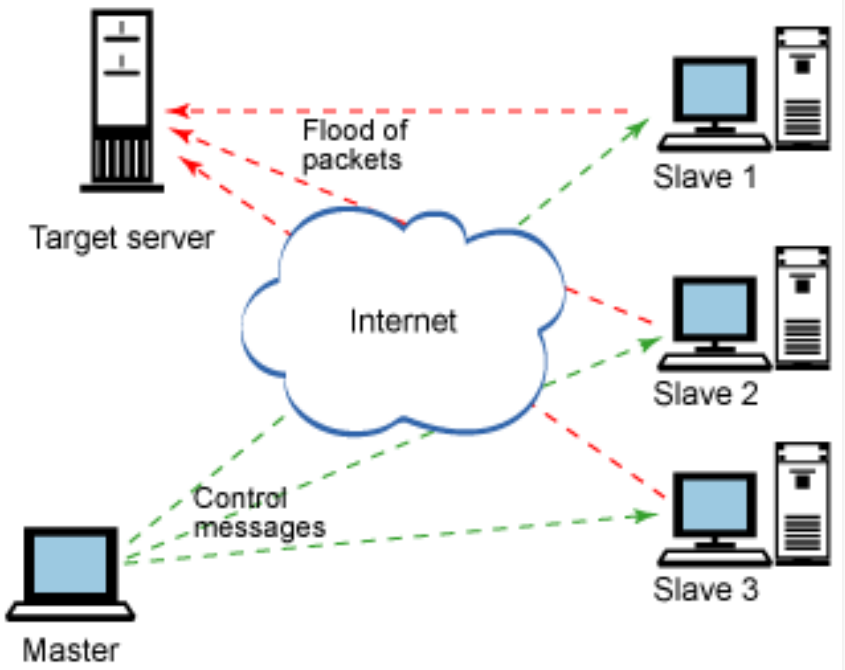
TCP/IP Vulnerabilities

- State Transitions
  - Unexpected
  - Security Overlooked
- Simultaneous Connection Establishment
- SYN Flooding
- SYN/FIN



Denial of Service

- Layered Attack
  - Physical, Network, Connection, Application
- LOIC
  - Distributed
- Financial Devastation
- Mission Disruption



www.ibm.com

IP Spoofing

- Masquerade as someone else
  - Identity theft for computers!
- Sequence Guessing
- Source Routing
- Connection Hijacking

IP V4/6

- IPv4
  - Small Address Space
  - No Authentication!
- IPv6
  - Sufficient Address Space
  - Secure Association
    - Authentication Headers
    - Encryption Headers
    - Session Key Exchange

No Strings Attached

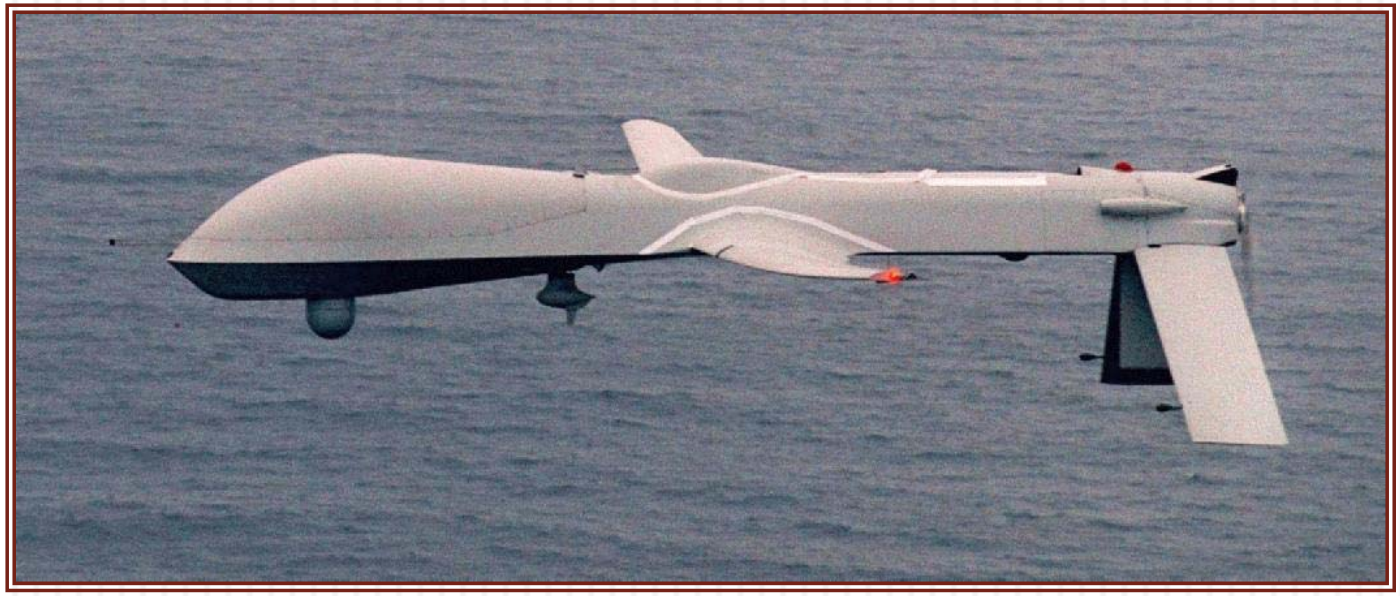
- How do these principles apply to the Wireless World?

Remember…

- …Wireless communications rely on the SAME underlying principles and protocols as wired communication
- Specific wireless applications only ADD vulnerabilities

What's the Big Deal?

Predator UAV

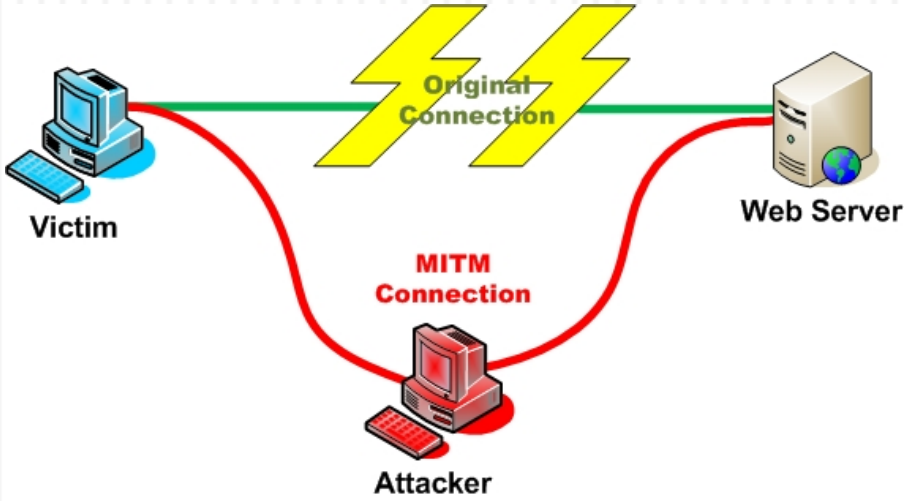


www.fas.org

Man-In-The-Middle

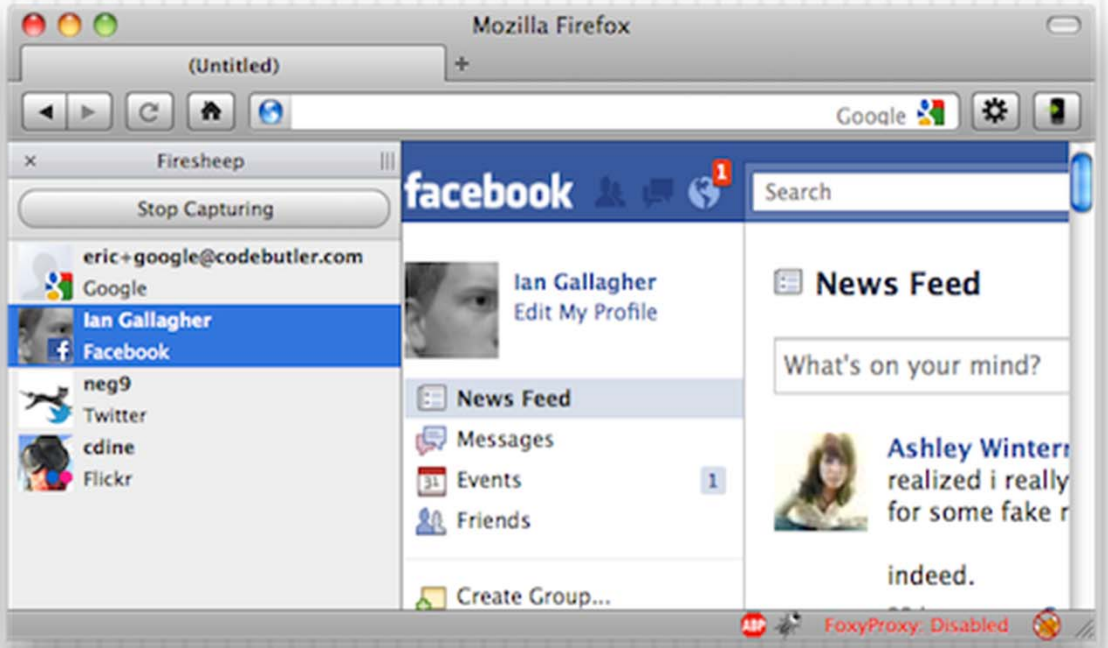
- IP Connection Hijacking
- BGP Prefix hijacking
- ARP Cache Poisoning

- Generally easier when wireless



www.owasp.org

802.11



- Wireless LANs
  - Open
  - WEP
  - WPA
- Firesheep
- Aircrack
  - Injection/Replay

Cellular

- Analog Signals
- Wearing a Wire
- Cloning
- Texting

- GSM
  - Broken

Bluetooth

- BlueJacking
- BlueSnarfing
- BlueBugging
- BlueDiving
- CarWhisperer
- BlueTooone
- Redfang

- bluez.org

Radio Frequency Identification

- Pro: Convenient for Tracking
  - Shipping Items
  - Inventory Control
- Con: Convenient for Tracking
  - Unique IDs for everything
  - Extensive Cross-Correlation
- Embed false data
- Battery Drain
- rfidiot.org

Location, Location, Location!

- GPS
- Wifi
- Mapping Services
- Smart Phones

- Is Privacy Dead?

Securing the Domain

Information Assurance, Best Practices, and Defense in Depth

The Cyber Battle…

- 1965… Password file vulnerability on IBM 7094
- 1988… Morris Worm
- 1995… US GAO says DoD computers hacked 250,000 times (about 65% successful)
- 1997… US Air Force base at Guam hacked
- 2007… Operation Orchard
- 2008… USB flash drive in Middle East
- 2009… Conficker worm
- Jan 2010… Operation Aurora
- Dec 2010… Operation Avenge Assange

This year…

- January 27-28… Egyptian blackout
- April 17… Sony Playstation outage
- September 26… Largest defacement in history… 700,000 websites
- October 16… *Sesame Street* You Tube channel hacked

This week…

- *Monday…* "Cyber Monday" – Over $1.25B in sales and more than 150 counterfeit websites seized
- *Tuesday…* ZoneAlarm reports…
  - More than 9 million Americans have their identities stolen each year
  - These identities are worth almost $5000 apiece to a criminal

Cyber Sabotage…
Touching the Physical World

- 1982… Soviet gas pipeline explosion

- September 2010… Stuxnet
- July 2011… Pentagon Cyber Strategy released…
  Cyber attack can be an act of war
- September 2011… DuQu

Credit: Rama/Creative Commons

- November 2011… Springfield, Illinois Water Plant

What do we do?

- Design in Information Assurance Fundamentals…
  - *Confidentiality*
  - *Integrity*
  - *Availability*
  - *Authentication*
  - *Nonrepudiation*
- Practice "Best Practices"
- Provide "Defense in Depth"

Information Assurance

- Confidentiality – Provide privacy for the sender and the receiver
  - The transmitted message should not be able to be read by a third party
  - Encryption at the sender and decryption at the receiver
    - Symmetric-key cryptography
    - Asymmetric-key cryptography
  - Requires key management

- Integrity – Data must arrive at the receiver exactly as it was sent by the sender – Free from tampering
  - Encryption and decryption provide secrecy, or confidentially, but not integrity
  - Achieved through the use of "hashing" – message is passed through a hash function that creates unique message digest

Information Assurance

- Authentication
  - *Message authentication* – Provides verification of the identity of the sender of the received message
    - Keyed hash functions – symmetric key approach
    - Digital signatures – asymmetric key approach
  - *Entity Authentication* – Identity of the user (entity) is verified prior to access to system resources
    - Something known only by the claimant (password, pin, etc.)
    - Something possessed by only the claimant (passport, ID card, etc.)
    - Something inherent to claimant (signature, fingerprints, retina pattern, etc.)
- Nonrepudiation – Prevents sender from denying having sent the message
  - Use of a trusted that archives the message and all supporting information
- Availability – Ensures service/access is not disrupted to users

Key Management

- Symmetric key distribution
  - Use a trusted center to reduce the number of keys required – all entities establish shared keys with the trusted center (key distribution center)
  - Trusted center issues symmetric "session keys" to be used for the duration of the session
- Assymetric key distribution
  - Again use a trusted center… but now the trusted center is a Certification Authority (CA)
    - Certificate associates public key with a specific entity – can be sure we have the right public key
  - Public Key Infrastructure (PKI)
    - Hierarchy of CAs – a higher level CA may not have the specific certificate, but can certify the lower CA

"Best Practices"

- Good reference… NSA recently published a set of best practices for home network security:

http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf

NSA: Best Practices for Keeping Your Home Network Secure (April 2011)

- Windows OS…
  - Migrate to modern OS and hardware platform
  - Install comprehensive host-based security suite
  - Limit use of administrator account
  - Use a web browser with sandboxing capability
  - Use a PDF reader with sandboxing capability
  - Migrate to Microsoft Office 2007 or later
  - Keep application software up-to-date
  - Implement full disk encryption (FDE) software

NSA: Best Practices for Keeping Your Home Network Secure (April 2011)

- Network Recommendations…
  - Home network design – use a separate (non-ISP provided) router
  - Implement WPA-2 on wireless network
  - Limit administration to internal network
  - Implement alternate DNS provider
  - Implement strong passwords on all network devices

NSA: Best Practices for Keeping Your Home Network Secure (April 2011)

- OPSEC/Internet Behavior…
  - Traveling with mobile devices – beware of hotspots
  - Exchanging home and work content – beware… home systems generally tend to be easier to compromise
  - Storage of personal information on Internet – know "the cloud" before you use it and periodically "google" yourself
  - Use of social networking sites
  - Enable the use of SSL encryption
  - E-mail best practices
  - Password management
  - Photo/GPS integration

NSA: Best Practices for Keeping Your Home Network Secure (April 2011)

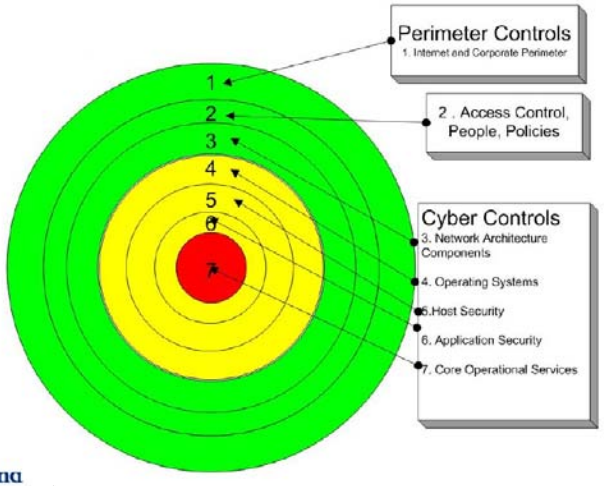
- Enhanced Protection…
  - Enhanced wireless router configurations…
    - MAC address filtering
    - Limiting the transmit power
    - SSID cloaking
    - Static IP addressing or limiting the pool of dynamic IP addresses
  - Disable scripting within the web browser
  - Enable Data Execution Protection (DEP) for all programs

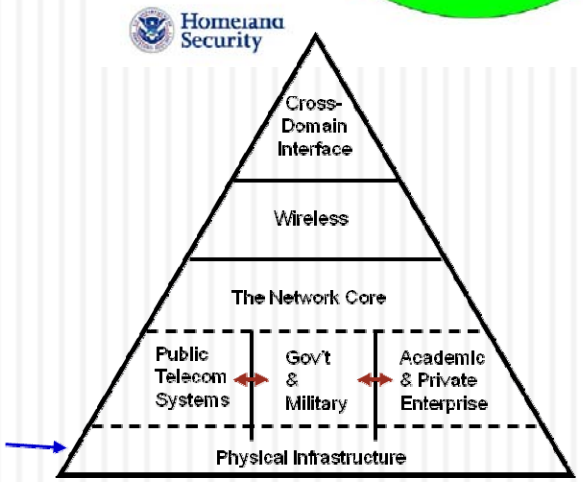
Available at:
http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf

Defense in Depth

- Policies and procedures
- Awareness and training
- Network segmentation
- Access control measures
- Physical security measures
- System hardening
- System monitoring

Edwards and Stauffer, Control System Security Assessments, *2008 Automation Summit*.





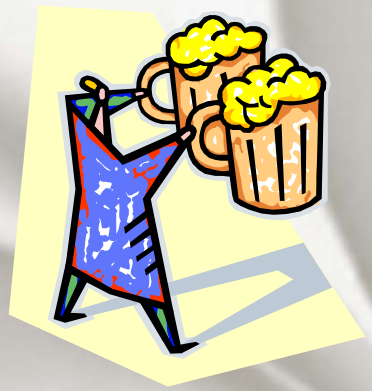
Open Research Questions
Wireless Level

- **Spectrum Dominance**
  - Can you incorporate spectrum management into network management?
  - Can you respect spectrum borders as well as physical borders?
- **Bandwidth and Data Management**
  - How do we manage the explosion of data (and bandwidth) required to operate Unmanned Systems?
    - Want human in the loop always (see: “The Matrix”, “The Terminator”, etc.)
  - Can we achieve Military QoS – 24/7/365, 100% utilization, >40 Mbps?

- **Tactical Communication Networks**
  - Can we harden Tactical Networks to cyberattacks?
    - Soldier must be able to fight when network is under attack.
    - Network must continue to operate when under attack.
  - Can system recognize cyberattack and avoid compromising physical domain? Can system authenticate physical devices via the network?
    - Hacker/virus launches ballistic missiles.
    - Take control/block control of unmanned asset.
    - Use SCADA to control allocation of physical resources.

Open Research Questions
Network Level

- **Communication and Routing Protocols**
  - Can we develop a protocol that can operate in a destabilized PHY layer?
  - Can we develop a means for Assured Information Exchange over a compromised network?
- **Resource and Overhead**
  - How do you do security with a battery?
  - How do you do security in a computationally constrained environment?
  - How do we maintain a good user experience (not every user needs a Ph.D. in EE to operate the system)?



Discussion to continue at the bar.

CYBER WARFARE IN THE WIRELESS WORLD

WHAT YOU DON'T KNOW *CAN* HURT YOU

LT D.A. Brown, CDR T.O. Walker, Ph. D., C. Anderson, Ph. D.
United States Naval Academy