University of Central Florida

INSTITUTE for SIMULATION & TRAINING

IDC 6601

Behavioral Aspects to Cybersecurity

"Cyber and Modeling and Simulation"

Bruce D. Caulkins, Ph.D.
Institute for Simulation and Training
University of Central Florida

Know Yourself!

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu, *The Art of War*

What are some examples of this in cybersecurity??

Definitions

Interdisciplinary approach to cyber and M&S

- Interdisciplinary - "…involving two or more academic, scientific, or artistic disciplines" (Merriam-Webster)
- Cyberspace - "…consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them." (JP 3-12R)

Definitions

Interdisciplinary approach to cyber and M&S

- Model - "a system of postulates, data, and inferences presented as a mathematical description of an entity or state of affairs" (Merriam-Webster)
- Simulation - "the imitative representation of the functioning of one system or process by means of the functioning of another" (M-W)

Disciplines in Cyber

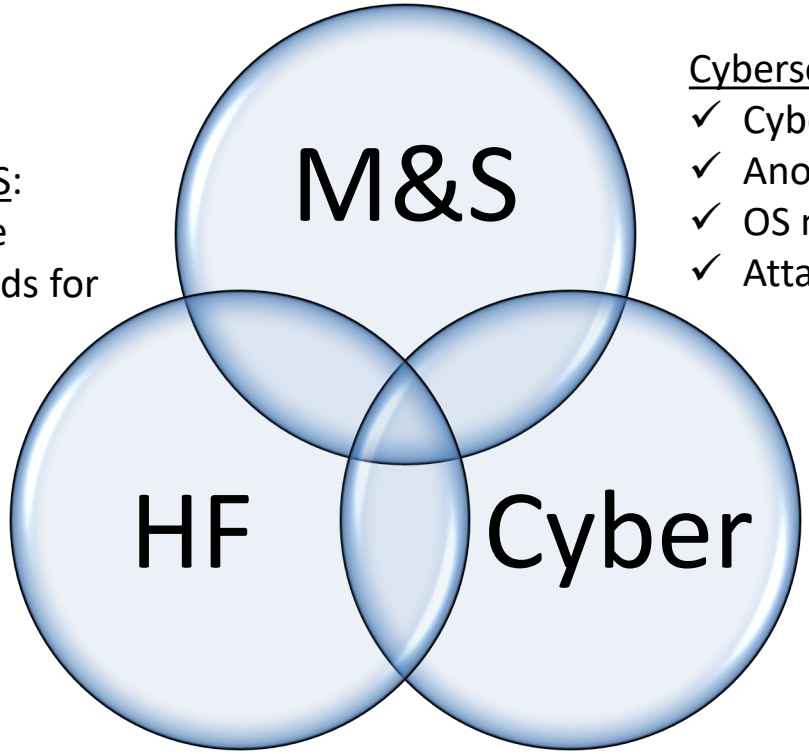
- Computer Science
- International Relations
- Human Factors
- Organization Strategy
- Data Mining
- Engineering
- Law
- Public Policy
- …others???

Disciplines in M&S

- Math, Statistics and Physics
- Industrial Engineering
- Human Factors
- Software Engineering
- Computer Science
- Digital Media

M&S of Behavioral Cybersecurity

Behavioral Aspects of M&S:
- ✓ Training & performance
- ✓ Interdisciplinary methods for problem solving
- ✓ Cognitive modeling
- ✓ HSI



Cybersecurity for M&S:
- ✓ Cyber ranges
- ✓ Anomaly detection
- ✓ OS modeling
- ✓ Attack vector simulation

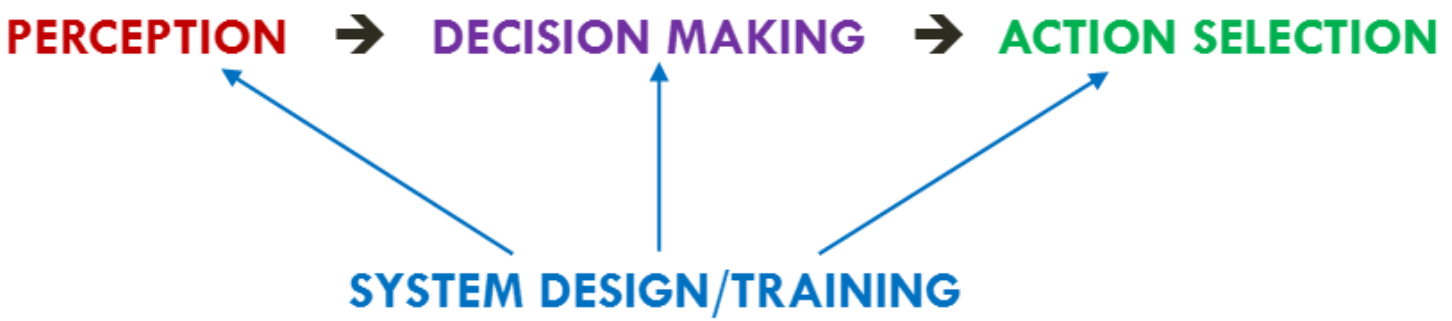
Behavioral Aspects of Cybersecurity:
- ✓ Insider threat detection
- ✓ Cyber workforce development
- ✓ Attack prediction
- ✓ Hacker motivations

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

1. What has Human Factors got to do with Cybersecurity?

"Scientific principles of ***perception***, ***decision making***, ***action selection***, and ***training*** that have been developed in basic and applied cognitive research….can provide a principled basis for analyzing the factors affecting security-related human decisions and choices" (Proctor & Chen, 2015, pp. 722)



Use phishing example with perception, DM etc

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

PERCEPTION

- Perception of information
- Views on security, risk perception (bias, heuristics)

DECISION MAKING

- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)
- Expert vs. novice decision making
- Bias and heuristics that affect decision making
- Decision making under stress, over/underload, fatigue

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

- Features of task, website etc.

TRAINING

- Organizational factors

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

PERCEPTION

- Perception of information
- Views on security, risk perception (bias, heuristics)

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

fatigue

What do you know about the perceived attack?
What are you biases? Are you a risk taker?

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

PERCEPTION

- Perception of information
- Views on security, risk perception (bias, heuristics)

DECISION MAKING

- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)
- Expert vs. novice decision making
- Bias and heuristics that affect decision making
- Decision making under stress, over/underload, fatigue

Are you an expert in this area? Is it a stressful situation? What other biases are at work here?

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

What course of action will you take? Is it the "easy road" or the most ambitious COA?

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

- Features of task, website etc.

TRAINING

- Organizational factors

Week 2's "Money" Slides

HUMAN FACTORS & CYBERSECURITY

What features of your operating system/operating environment allowed you to come to this decision? What training helped you?

ACTION SELECTION

- Ease of implementing response

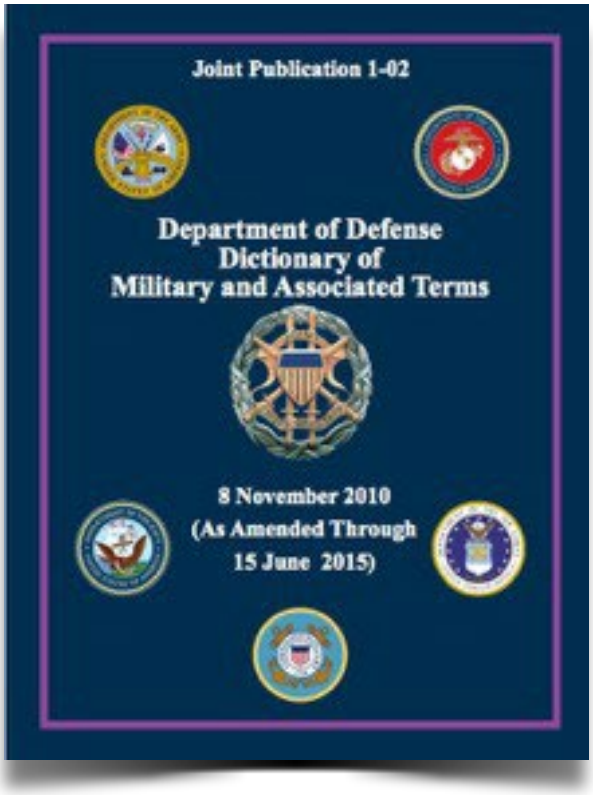
SYSTEM DESIGN

- Features of task, website etc.

TRAINING

- Organizational factors

Vulnerability of Information System



"… a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system." - JP 1-02

Cyber Actors

White Hat Hackers

Black Hat Hackers

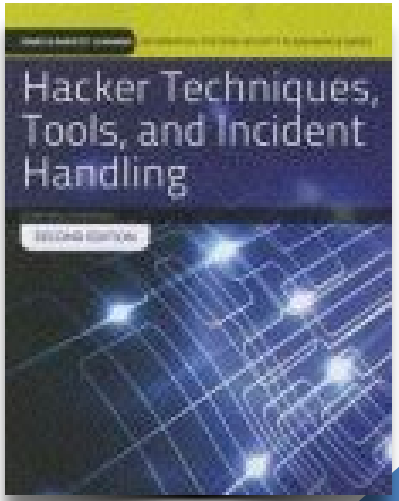
Gray Hat Hackers

So how do these actors conduct their work?

Suicide Hackers

Script Kiddies

Common Hacking Methodologies



Planting Backdoors

Covering Tracks

Escalation of Privilege

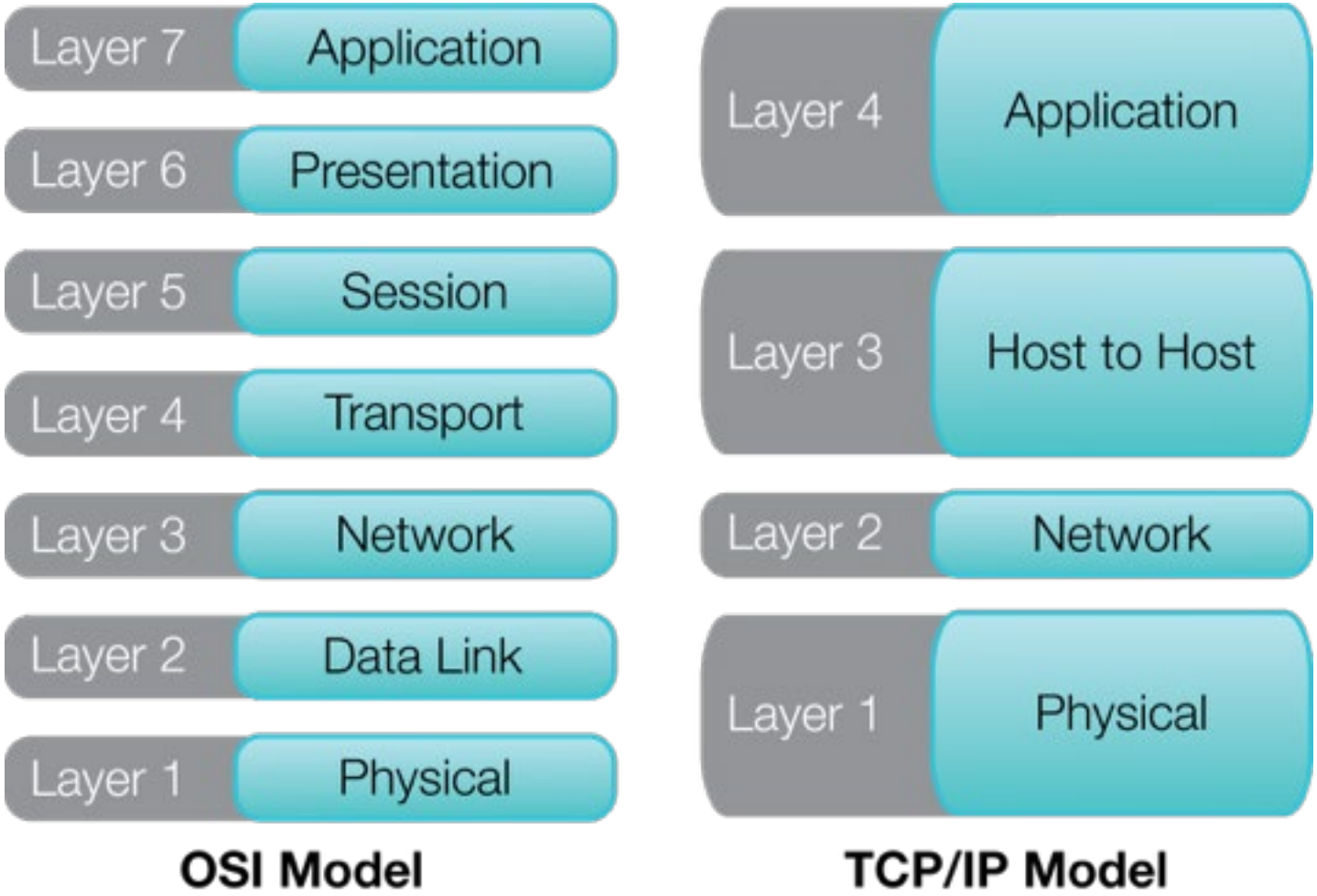
System Hacking

Enumeration — *gathers more info like usernames*

Scanning — *more active like ping*

Footprinting — *passive query like whois*

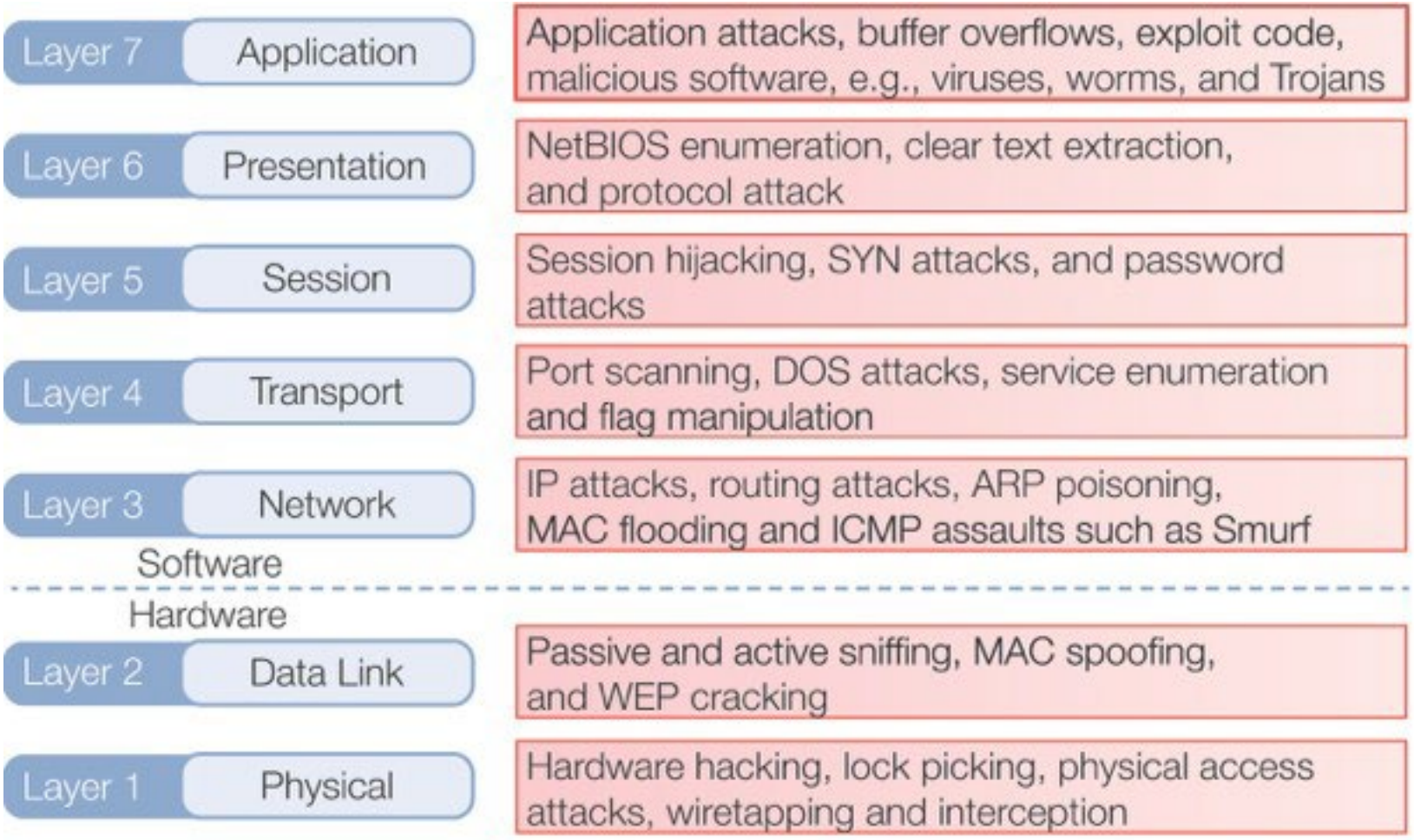
OSI Reference Model vs. TCP/IP Model



Mapping OSI Layers to Protocols

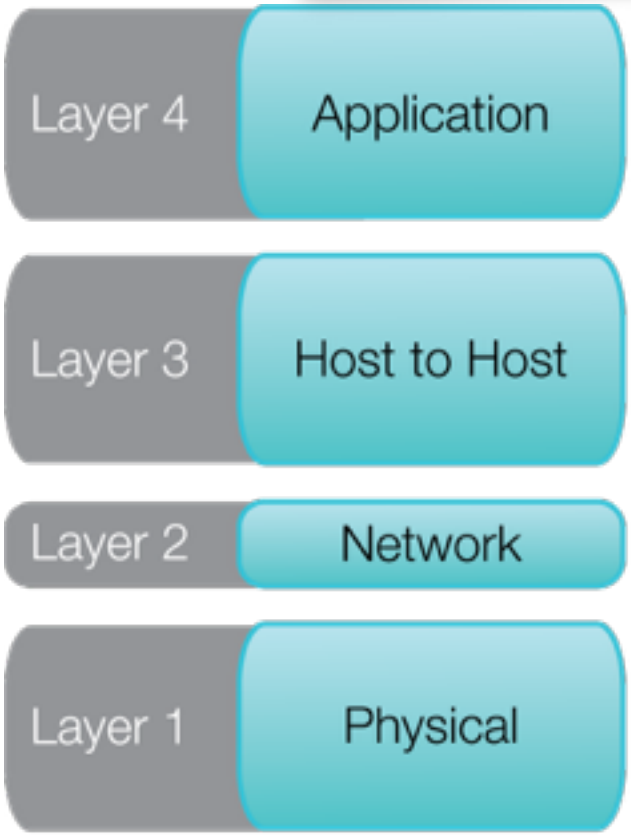
OSI REFERENCE MODEL LAYER	COMMON PROTOCOLS AND APPLICATIONS
Application	FTP, TFTP, SNMP, Telnet, HTTP, DNS, and POP3
Presentation	ASCII, EBCDIC, TIFF, JPEG, MPEG, and MIDI
Session	NetBIOS, SQL, RPC, and NFS
Transport	TCP, UDP, SSL, and SPX
Network	IP, ICMP, IGMP, BGP, OSPF, and IPX
Data Link	ARP, RARP, PPP, SLIP, TLS, L2TP, and LTTP
Physical	HSSI, X.21, and EIA/TIA-232

OSI Layers and Attacks

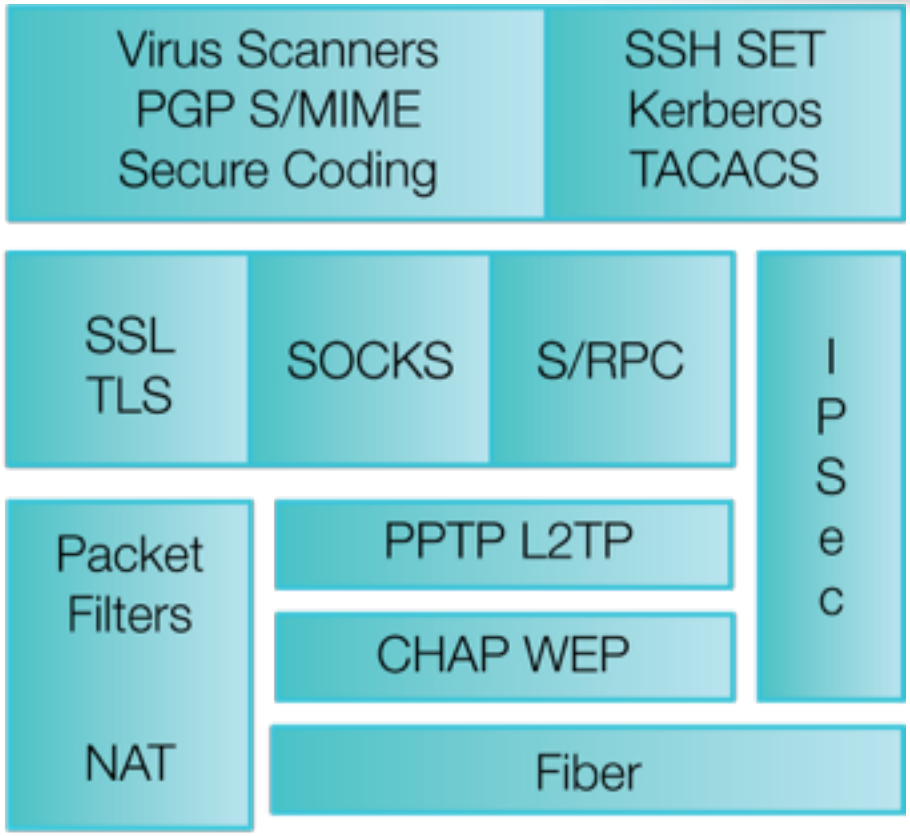


TCP/IP Model Layer Controls

What do many of these controls have in common??



TCP/IP Model



Controls and Countermeasures

Cryptography

- Protection and preservation of information
- Encrypted messages still can be intercepted; but they cannot* be read by interceptor
- Examples include:
  - Secure Sockets Layer (SSL)
  - Secure Shell (SSH)
  - Pretty Good Privacy (PGP)
  - Wi-Fi Protected Access (WPA)
  - Internet Protocol Security (IPSec)

In Summary, part 1…

- Cyber continues to grow in importance
- Security techniques continue to be taught at all levels
- Military and civilian applications are extensive
- Cyber is increasingly being used for education and training in the military and commercial industry
- The use of cyber ranges is increasing for students of all ages and educational levels
- Legal and privacy issues are increasingly important
- Governments are looking more towards whole-of-government (WoG) approaches to cyber

In Summary, part 2…

- Simulation is gaining recognition as an scientific field with a core body of knowledge being developed
- Simulation is being taught to students from high school through graduate school
- Simulation is increasingly being used for education and training in many applications, e.g., medicine and the military
- The use of simulation games is increasing for students of all ages and educational levels
- M&S is emerging as an academic field
- Simulation is cost-effect in many applications
- The M&S industry is growing

Some Parting Thoughts - Cyber and M&S

- Cyber is an operational domain in the military
- M&S is a separate and distinct career area and industrial endeavor supported by an emerging academic discipline
- Cyber continues to expand in importance due to our reliance on technology
- Growth in M&S (as well as simulation-based training-MS&T) will support a growing enterprise
- Military M&S and cybersecurity will maintain its steady growth; other areas, such as simulation for entertainment and medical training will grow rapidly

University of Central Florida

INSTITUTE for SIMULATION & TRAINING

IDC 6601

Behavioral Aspects to Cybersecurity

"Cyber and Modeling and Simulation"

Bruce D. Caulkins, Ph.D.
Institute for Simulation and Training
University of Central Florida