INFORMATION

The 15th Annual

Cybersecurity Day at IUP

October 18, 2022
TIME: 9:00 A.M. — 4:00 P.M.

OHIO—HUB (319 Pratt Drive, Indiana PA 15705)

Featuring:

A Number of Recognized Security Experts from Academia, Industry, and Government

For More Information, Please visit the Institute for Cybersecurity Site:

http://www.iup.edu/cybersecurity/

Open to IUP Students, Faculty, Staff and all Community Members

IUP

15th ANNUAL
CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00 – 9:05 am	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Introduction
9:05 – 9:10 am	Lara Luetkehans, IUP's Provost and Vice President for Academic Affairs	Provost Remarks
9:10 – 9:15 am	Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics	Opening Remarks
9:15 – 9:20 am	Francisco E. Alarcon, Chair, Department of Mathematical and Computer Sciences	Welcome Message
9:20 – 9:30 am	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Event history, ICS work, and recent achievements, and logistics
9:30 – 10:15 am	Dr. Rita Doerr, Academic Outreach Lead, National Security Agency	Countermeasures and Risk Management: A Principled Approach
10:20 – 11:05 am	Ms. Mackenzie Monarko, Special Agent & Private Sector Coordinator, FBI Pittsburgh	From Gang Busters to Ransomware Gangs: Evolution of FBI Investigations
11:10 – 11:55 am	Mr. Christopher May, Technical Director, Cyber Workforce Development, CERT® Division, Software Engineering Institute, Carnegie Mellon University	Become a Cyber Warrior for Free, Courtesy of Uncle Sam!
12:00 – 1:15 pm	Lunch Break	
1:15 – 2:00 pm	Dr. Bryant Wysocki, Senior Level Executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Air Force Research Laboratory, Rome NY	Information Warfare
2:00 – 2:10 pm	Afternoon Break	
2:10 – 2:55 pm	Mr. Nigel Wright, Director of Product for Locomation	Designing Systems for Security: Walls are Only as Secure as They are Designed
2:55 – 3:05 pm	Afternoon Break	
3:05 – 3:50 pm	Panel Discussion, Amanda Marshall, Dan Yuhas, Bill Balint	Multi-Factor Authentication: A Cybersecurity Difference Maker
3:50 – 4:00 pm	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Conclusions

BIO INFO CONTINUED

Amanda Marshall, Director, Project Management, IUP

Amanda L. Marshall, director, Project Management, Indiana University of Pennsylvania. Marshall received her BS in management information systems from IUP in 1996. She began her career as a help desk technician for Commonwealth Systems Corporation. Amanda has held several technology positions at IUP, including technology support analyst, coordinator of user services, and, most recently, director of project management for IT Services. One of the most recent projects Amanda has been tasked with is the implementation of DUO, IUP's multifactor authentication service. She is also instrumental in IUP cybersecurity initiatives. Amanda communicates regularly with the IUP community by alerting users to phishing and scam alerts and by providing information and tips to educate users on the importance of cybersecurity.

Dan Yuhas, Director, IT Compliance and Administration, IUP

Daniel J. Yuhas, director, IT Compliance and Administration, Indiana University of Pennsylvania. Yuhas received his BS in computer science from IUP in 1988. He began his career as a software engineer for Vitro Corporation designing tactical weapons systems for the US Navy. He has held a variety of technology positions at IUP for 32 years, including director of Research and Development and director of Instructional and Research Technologies. He currently serves as director of IT Compliance and Administration focusing on IT compliance, cybersecurity, IT strategy, IT governance, IT policy, contracting, and personnel and financial management.

Bill Balint, Chief Information Officer, IUP

Bill Balint has 34 years of IT experience and became IUP's chief information officer in 2006. Bill has presented at more than 50 industry events at the regional, state, national, and international levels and has authored, co-authored, or been interviewed for more than 35 publications and websites via written, audio, and video formats. He is also a member of the Pittsburgh Executive CIO governing board.

GUEST SPEAKER TITLES AND ABSTRACTS

Rita Doerr, Academic Outreach Lead, National Security Agency
Title: Countermeasures and Risk Management: A Principled Approach
Abstract: Countermeasures are any actions, devices, procedures, techniques, or other measures that reduce the vulnerability of any information system. In this presentation, we provide a principled approach to using countermeasures when attempting to thwart cyber adversarial attacks. We will address several techniques that will help to reduce and mitigate impact through the principles of Defense in Depth and Least Privilege, and briefly speak to how one must remain ever vigilant.

Mackenzie Monarko, Special Agent & Private Sector Coordinator, FBI
Title: From Gang Busters to Ransomware Gangs: Evolution of FBI Investigations
Abstract: This talk will explore the history of the FBI and walk the participants through the progression of FBI investigations from traditional criminal matters to modern day cyber and counterintelligence investigations. Criminals, regardless of their level of sophistication, are leveraging technological advances to evade detection by law enforcement. Some actors, whether they are financially motivated or nation-states, use a vast array of skills to hide within corporate networks to steal data or intellectual property. This talk will highlight how knowledge and understanding of computer science and information systems and being "tech savvy" are useful to advance investigations.

Christopher May, Technical Director, Cyber Workforce Development, CERT® Division, Software Engineering Institute, Carnegie Mellon University
Title: Become a Cyber Warrior for Free, courtesy of Uncle Sam!
Abstract: This talk will showcase and demonstrate technologies and methods for rapidly enhancing and assessing the skills and experience-level of aspiring cyber operators and defenders. The CERT® division of Carnegie Mellon University's Software Engineering Institute develops cutting-edge cyber training platforms, simulators, and hands-on content in support of the U.S. Department of Defense and the U.S. Cybersecurity and Infrastructure Security Agency (CISA). These capabilities were recently released as open-source software and are used for U.S. Indo-Pacific Command's Cyber Endeavor exercise, the U.S. Army's Gaining Cyber Dominance program and the White House sponsored President's Cup Cybersecurity Competition. The presenter will discuss how organizations can easily leverage these freely-available tools to jump start or enhance their own training, testing or security research programs.

Bryant Wysocki, Senior Level executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory, Rome, NY
Title: Information Warfare
Abstract: Technology is advancing at speeds beyond previous human experience and nowhere is this more evident than in cyber information systems. The resulting information flow fuels our global economy, has altered world cultures, and serves as critical infrastructure within society and national security. Our information dependencies go deep making the assurance of cyber dependent missions a national priority. This talk examines the evolving challenges connected to protecting information in an increasingly fast paced and complex landscape where cyber capabilities converge with other more traditional means of national defense. The material introduces operational concepts related to information assurance and the four pillars of information warfare while considering the attributes of a stable and resilient information infrastructure.

Nigel Wright, Director of Product for Locomation
Title: Designing Systems for Security: Walls are only as secure as they are designed
Abstract: In any industry, proper system design will be the difference between success and failure. Allocation of system features, design of data elements, and thoughtful consideration of tradeoffs must occur to ensure that the product is secure, robust and reliable at the end of the day. Participants will learn about historical failures of secure system designs made by teams choosing the wrong incentives and understand how these factors will impact them in the real world in this engaging presentation

Panel Discussion: Amanda Marshall, Dan Yuhas, Bill Balint
Title: Multi-Factor Authentication: A Cybersecurity Difference Maker
Abstract: This panel discussion will provide attendees with a working knowledge of multifactor authentication (MFA) and to explain its purpose as part of a cybersecurity program. Attendees will learn why MFA is helpful, how it works, its benefits and challenges and various other related information

For more information about Cybersecurity Day at IUP, please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu, 724-357-7995.

THE 15TH ANNUAL

CYBERSECURITY DAY AT IUP

OCTOBER 18, 2022

OHIO HUB
IUP MAIN CAMPUS

CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00 – 9:05 am	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Introduction
9:05 – 9:10 am	Lara Luetkehans, IUP's Provost and Vice President for Academic Affairs	Provost Remarks
9:10 – 9:15 am	Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics	Opening Remarks
9:15 – 9:20 am	Francisco E. Alarcon, Chair, Department of Mathematical and Computer Sciences	Welcome Message
9:20 – 9:30 am	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Event history, ICS work, and recent achievements, and logistics
9:30 – 10:15 am	Dr. Rita Doerr, Academic Outreach Lead, National Security Agency	Countermeasures and Risk Management: A Principled Approach
10:20 – 11:05 am	Ms. Mackenzie Monarko, Special Agent & Private Sector Coordinator, FBI Pittsburgh	From Gang Busters to Ransomware Gangs: Evolution of FBI Investigations
11:10 – 11:55 am	Mr. Christopher May, Technical Director, Cyber Workforce Development, CERT® Division, Software Engineering Institute, Carnegie Mellon University	Become a Cyber Warrior for Free, Courtesy of Uncle Sam!
12:00 – 1:15 pm	Lunch Break	
1:15 – 2:00 pm	Dr. Bryant Wysocki, Senior Level Executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Air Force Research Laboratory, Rome NY	Information Warfare
2:00 – 2:10 pm	Afternoon Break	
2:10 – 2:55 pm	Mr. Nigel Wright, Director of Product for Locomation	Designing Systems for Security: Walls are Only as Secure as They are Designed
2:55 – 3:05 pm	Afternoon Break	
3:05 – 3:50 pm	Panel Discussion, Amanda Marshall, Dan Yuhas, Bill Balint	Multi-Factor Authentication: A Cybersecurity Difference Maker
3:50 – 4:00 pm	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	Conclusions

BIOGRAPHICAL INFORMATION ON GUEST SPEAKERS

Rita Doerr, Academic Outreach Lead, National Security Agency

Rita Doerr has been employed as a Computer Scientist with the National Security Agency (NSA) for over 37 years. She is currently the Academic Outreach Lead for the Cybersecurity Directorate's (CSD) Cybersecurity Collaboration Center. Prior to her arrival in CSD, she was a Cyber Instructor within NSA's National Cryptologic School's College of Cyber. During this assignment, Dr. Doerr completed a 3 year technical development program focusing on cybersecurity education and training where she toured in NSA's Red Team and Academic Engagement Offices. Her external tours included teaching at Archbishop Spalding High School and the University of Maryland, Baltimore County's CSEE Graduate Program, and serving as a cyber consultant for the Maryland Air National Guard's 175th Cyberspace Operations Group.

Mackenzie Monarko, Special Agent & Private Sector Coordinator, FBI

Special Agent Mackenzie Monarko joined the FBI in 2006 and is currently assigned to the FBI Pittsburgh Division. Her previous office assignments included Albuquerque and Philadelphia, and she has worked a variety of investigations to include violent gangs, organized crime, international and domestic terrorism, and criminal cyber matters. In January 2021, SA Monarko took on the role of Private Sector Coordinator where she works closely with Cyber and Counterintelligence Agents and Intelligence Analysts to keep organizations apprised of priority threat intelligence.

Christopher May, Technical Director, Cyber Workforce Develpment, CERT@ Division, Software Engineering Institute, Carnegie Mellon University

Christopher May is a technical director within the CERT® Division of Carnegie Mellon University's Software Engineering Institute. In this role, he leads a team of over 60 cybersecurity researchers in developing the technical abilities of the U.S. military's cyber operators. Additionally, he founded the Cyber Forensics and Incident Response curriculum track within CMU's Information Security master's degree program, and taught courses therein for 17 years. Prior to joining Carnegie Mellon, May served 7-years as a US Air Force communications officer.

Bryant Wysocki, Senior Level Exec, Technical Advisor for C4I and Cyber Systems for the Air Force, Associate Director, Information Directorate, Air Force Research Laboratory.

As the recognized national/international authority on C4I and cyber systems, Wysocki provides technical oversight of these areas for the Air Force and advice on C4I and cyber systems to the highest level Air Force and government officials. Wysocki evaluates technical approaches and develops transition strategies for directorate technologies and serves as the senior scientist liaison to external national and international partners across government, academia, and industry. Wysocki started his active duty career with the Air Force as a nuclear weapons technician in 1991 and served in numerous technical and operational positions throughout his service as a development engineer and later as a civilian scientist. Wysocki is a retired Air Force officer with experience in industry, academia and government. He has a broad span of technical leadership experience with a diverse background in military operations, acquisitions, logistics, maintenance, program management, systems engineering, engineering physics, fundamental research, and technology development.

Nigel Wright, Director of Product for Locomation

Nigel Wright is an alumnus of California University of Pennsylvania and an advocate for reliable, safe, and secure automated systems. Wright has spent his career developing safety critical autonomous systems and currently serves as Director of Product for Locomation. Responsible for Product initiatives & strategy, Wright works with the team to ensure that the human lead convoy delivers safe, consistent, reliable performance generating value for the end customers. Wright also supports the advisory boards for Indiana University of Pennsylvania and Pennwest at California, providing support for curriculum development. Wright holds a Bachelor's Degree in Computer Engineering Technology from California University of Pennsylvania, a Master's Degree in Business Administration from Point Park, and has completed executive post graduate education in Software Architecture (Carnegie Mellon University Software Engineering Institute), Model Based System Engineering with (MITx), Innovation Management (Villach, Austria) and Leadership and Culture (Harvard University in partnership with Uber).

Countermeasures: A Principled Approach

Rita M. Doerr, Ph.D.
Academic Outreach Lead
Cybersecurity Directorate
National Security Agency

Module 3 – Countermeasures and Risk Management

Three Principles

How to reduce risk and mitigate impact:

- Principle 1: **Defense in Depth**
- Principle 2: **Least Privilege**
- Principle 3: **Vigilance**

Module 3 – Countermeasures and Risk Management

Principle 1 – **Defense in Depth**

Every system and network should have multiple layers of defense against intrusion.

Module 3 – Countermeasures and Risk Management

Principle 1 – **Defense in Depth**

Uses multiple security controls throughout a defended network in a layered approach

- **Example:** Multiple firewalls, anti-malware installed on both servers and workstations, and so on
- Also called the "castle defense"

Historical and military precedents:

- Layered defense (multiple lines of defense)
- Delays the enemy's advance and inflicts losses via attrition
- Opposed to a "crust defense"

Module 3 – Countermeasures and Risk Management

Principle 1 – Defense in Depth

Specific Countermeasures

- Firewalls
- Demilitarized Zone (DMZ) or Perimeter Network
- Private Addressing and Network Address Translation (NAT)
- Proxy Servers
- Data Encryption
- Input Validation
- Content Protection
- Anti-Malware Controls
- Configuration Management

Firewalls

A *firewall* monitors and filters network traffic

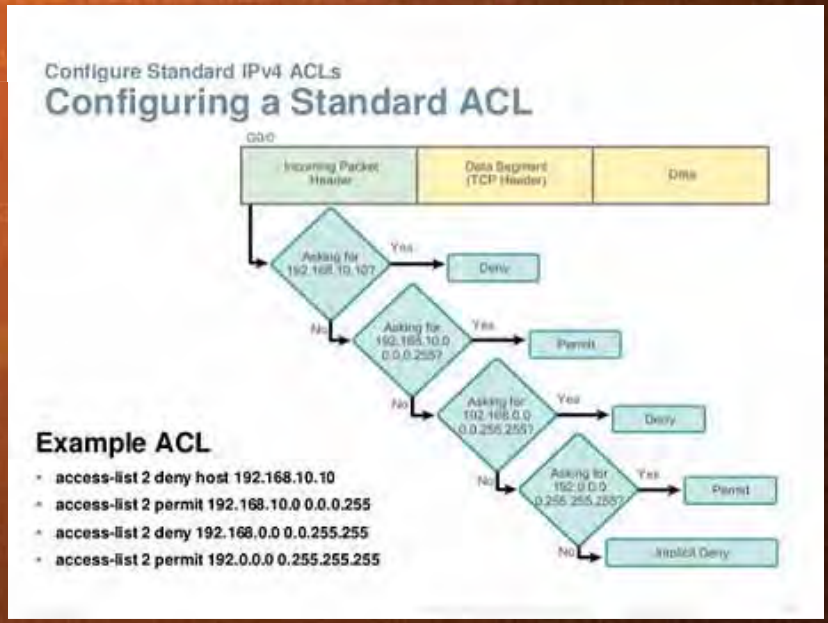
- Applies pre-defined rules
  - First generation: packet filters
  - Second generation: “stateful” packet filters
  - Third generation: application-aware firewalls
- Can filter inbound or outbound traffic
- Can be network-based or host-based

Module 3 – Countermeasures and Risk Management

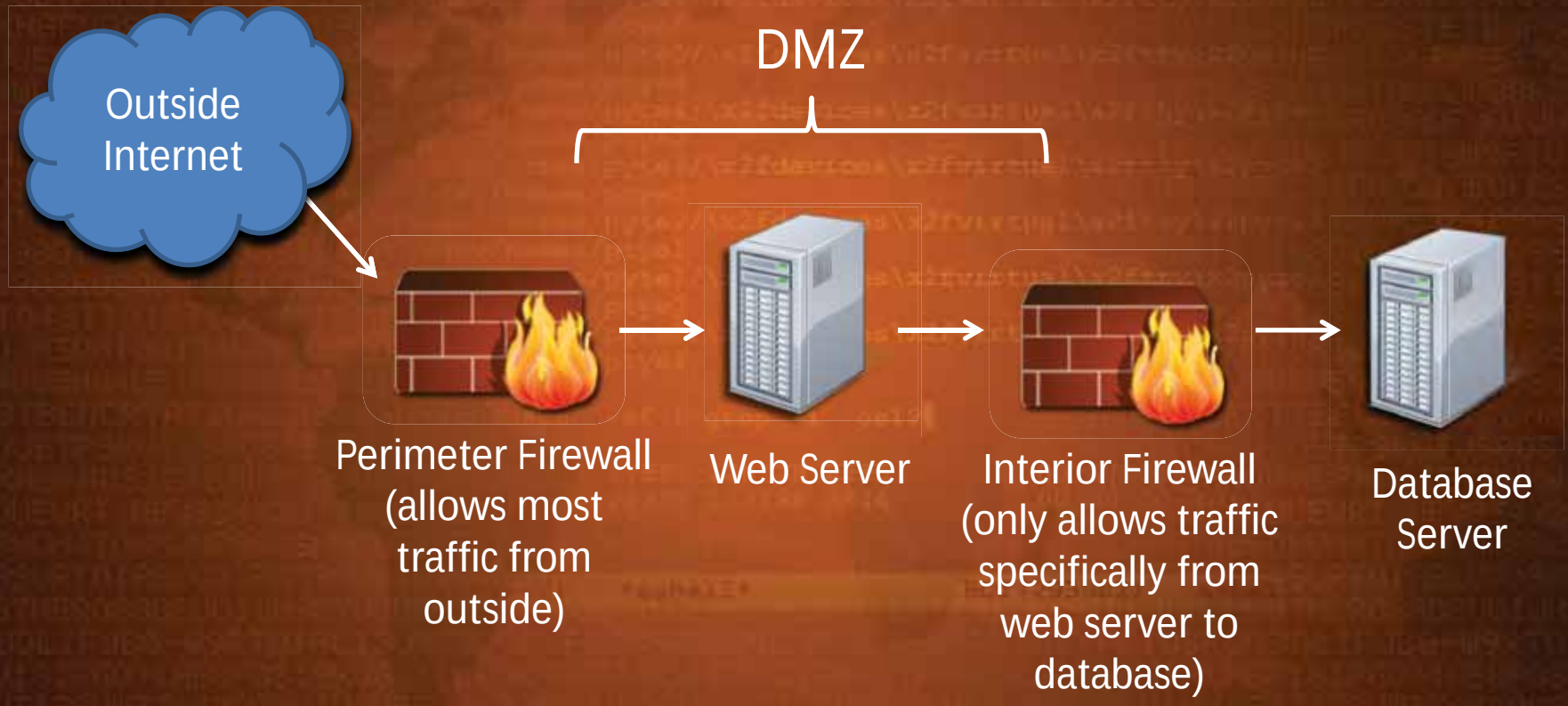
Firewalls

Can be applied in a variety of ways

- Permit communication only from or to trusted entities
- Permit communication only on essential channels or “ports”
- Time out repeated connections from the same source
- Flag or discard suspicious data



Demilitarized Zone (DMZ) or Perimeter Network



Private Addressing

Private addresses are used inside enclave networks

- Intended to mitigate problem of "running out of IP addresses"
- Packets with private addresses are *dropped* by public routers
- Different enterprises can use the same private addresses

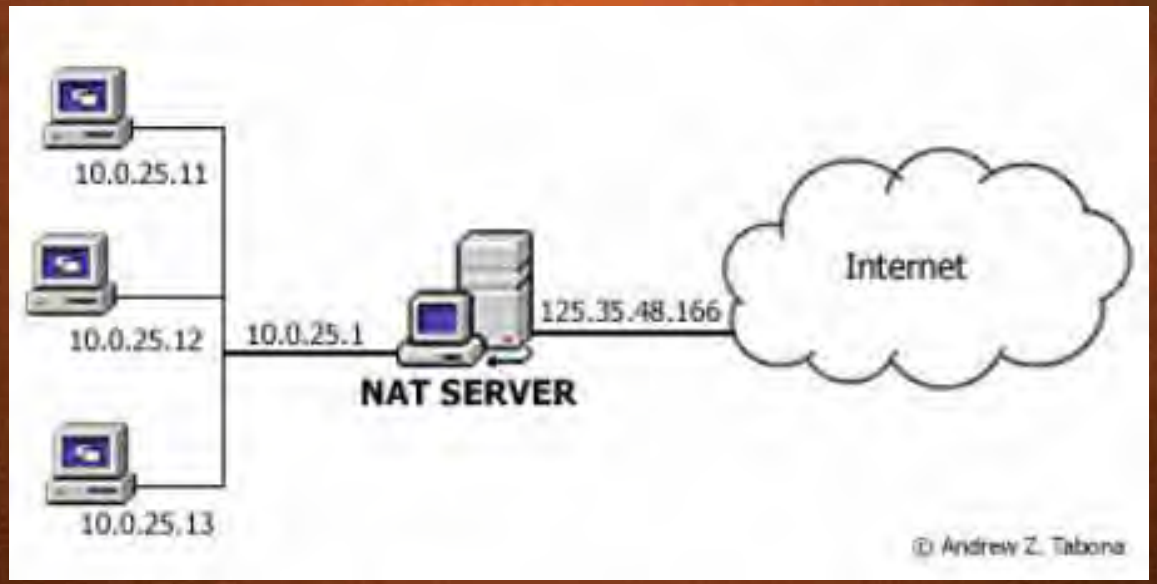
Block Size	First IP Address	Last IP Address	TOTAL
16-bit block	192.168.0.0	192.168.255.255	65,536
20-bit block	172.16.0.0	172.31.255.255	1,048,576
24-bit block	10.0.0.0	10.255.255.255	16,777,216

- **Not very useful by itself . . .**

Network Address Translation (NAT)

Network addresses of packets are modified in transit

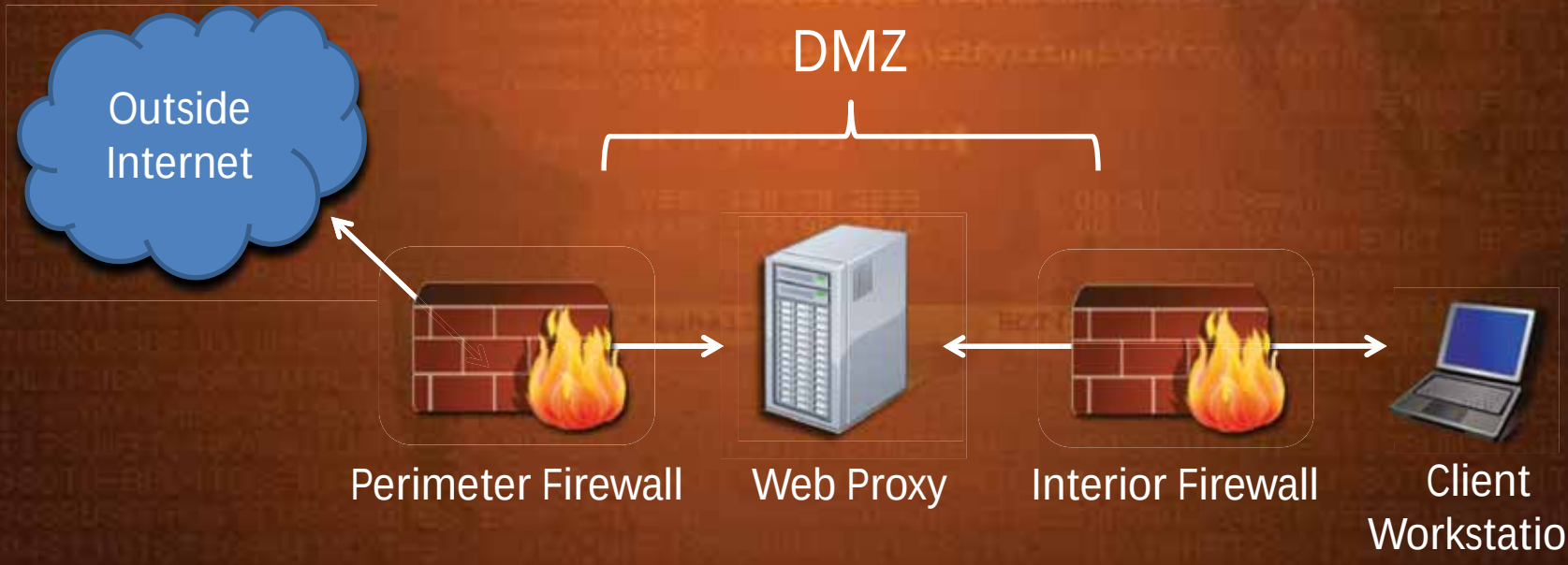
- Entire enclave network can share a single public IP address
- Can be used to obscure the actual addressing scheme of the network



Proxy Servers

Client requests can be routed through a *proxy server*

- Most proxy servers are for web traffic
- Server can simplify and bundle client requests
- Server can also *filter* outbound requests or inbound data



Blacklisting and Whitelisting

Blacklisting: make a list of addresses, sites, applications, or other entities which are *forbidden* to communicate

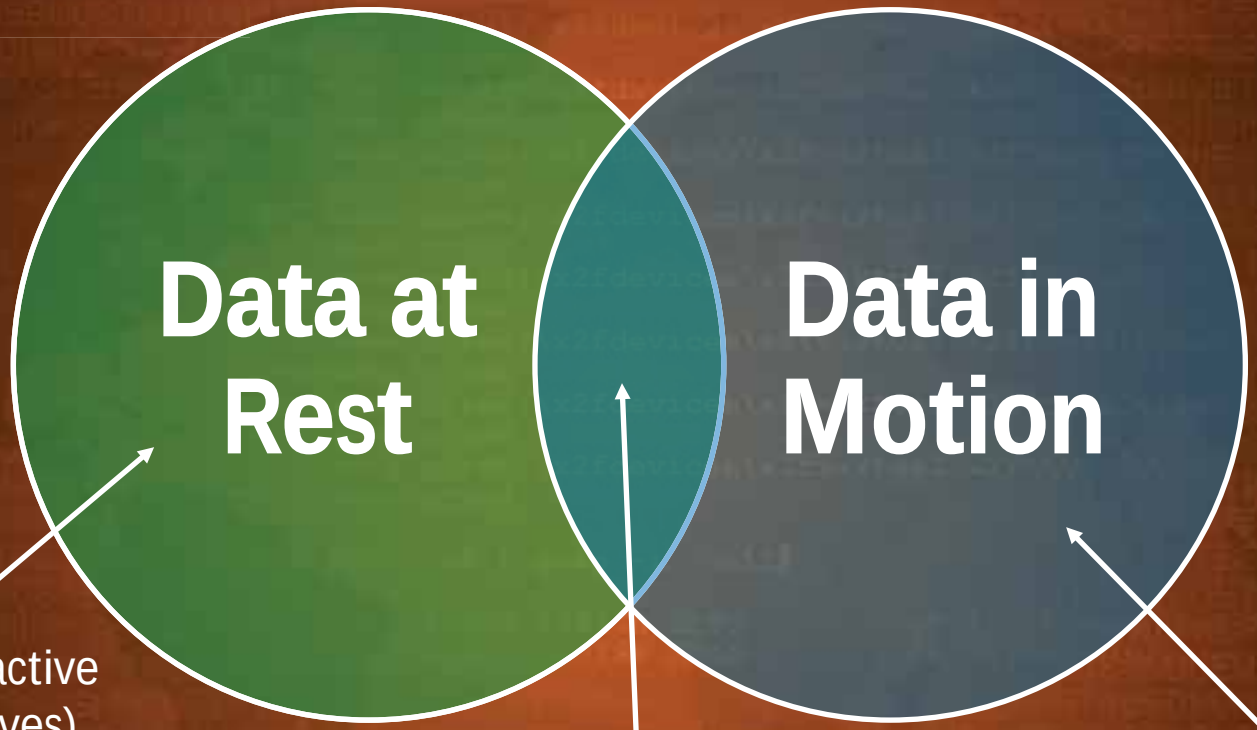
- "Everything not specifically forbidden is allowed"
- Requires that you know sources of malicious data or activity
- Can easily be applied reactively

Whitelisting: make a list of addresses, sites, applications, or other entities which are *permitted* to communicate

- "Everything not specifically allowed is forbidden"
- Requires that you know everything you need for mission

Most effective strategies involve both

Data Encryption



Data Encryption

Data at rest can be either:

- *Unstructured* – in files and storage
- *Structured* – in databases or applications

In either case, use **strong encryption** (AES, RSA, SHA-256)

Data in motion should be protected using *secure protocols:*

For . . .	Instead of using . . .	Use . . .
Web Access	HTTP	HTTPS
File Transfer	FTP, RCP	FTPS, SFTP, SCP
Remote Shell	telnet	SSH2 terminal
Remote Desktop	VNC	radmin, RDP

Internet Protocol Security (IPSec)

Suite for secure Internet Protocol (IP) communications

- Applies both authentication and strong encryption
- Can work host-to-host or enclave-to-enclave
- Difficult to set up correctly but *very effective*

Input Validation

Check any user-provided data for validity

- Does the data make sense for the field where it was entered?
- Will the data cause an inappropriate action?

Content Protection

Content that doesn't change can be made **unmodifiable**

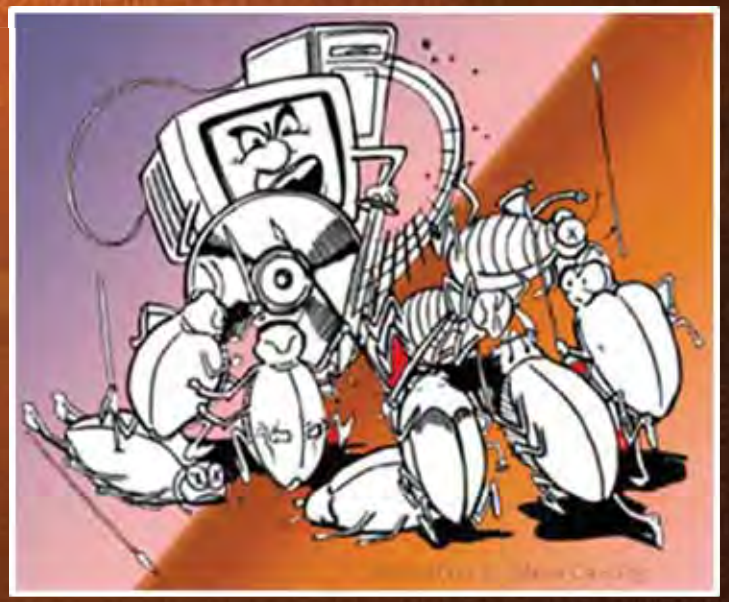
- File system protections . . .
- Or run your website from read-only media!

Encode scripts so an adversary can't easily read them

Anti-Malware Controls

Software examines inbound data for evidence of malware

- "Signatures" or strings of data from known malware
- Connections to suspicious sites
- Unexpected system behavior
- Can operate as a host-based firewall



Patch Management

Patch: an incremental update to software to fix a bug or vulnerability in the code

- Usually distributed for free to legitimate customers
- May be released on a regular schedule ("Patch Tuesday")
- Presents a challenge on large or heterogeneous networks
- Not useful against zero-day exploits

Still one of the most effective countermeasures against hostile network intrusion!

Module 3 – Countermeasures and Risk Management

Configuration Management

Make sure systems are configured to be as secure as possible – they aren't necessarily so "out of the box"

Examples:

- Disable automatic execution of macros in documents
- Disable HTML links in emails
- Disable ICMP ("ping") responses
- Disable "promiscuous" mode on network interfaces
- Control the proliferation of trust relationships
- Force periodic re-authentication and session timeouts

Look for the *configuration guide* for your OS or application!

Module 3 – Countermeasures and Risk Management

Configuration Management – Banner Obfuscation

Many servers respond with a *banner* when queried:

```
HTTP/1.1 302 Found
Date: Wed, 04 Dec 2013 16:34:43 GMT
Server: Apache/2.2.16 (Debian)
```

```
220 mail.utopia.org ESMTP Sendmail 8.13.8/8.14.2
```

Intruder can use these to identify vulnerabilities

Banner is usually configurable:

```
HTTP/1.1 302 Found
Date: Wed, 04 Dec 2013 16:34:43 GMT
Server: Generic Web Server
```

Module 3 – Countermeasures and Risk Management

Principle 2 – **Least Privilege**

No account or process on a system should have access to any functions or information it does not need in order to carry out its legitimate function.

Principle 2 – **Least Privilege**

Restricts the *privileges* available to each account or process

Limits the scope of any security control exception

Advantages:

- Makes system or network defense easier to plan
- Limits the damage if the account or process is compromised
- Makes any given intrusion easier to contain

Principle 2 – Least Privilege

Specific Countermeasures

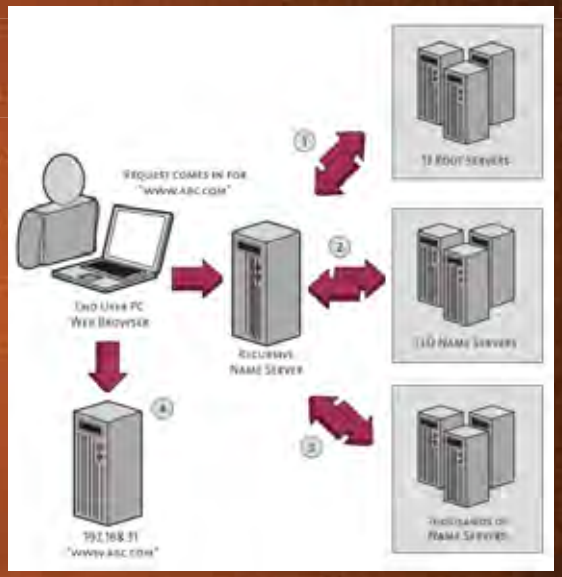
- Removing Unnecessary Accounts and Services
- Minimizing Processes with Elevated Privileges
- Sandboxing Servers
- Separation of Duties

Module 3 – Countermeasures and Risk Management

Removing Unnecessary Accounts and Services

Every service and account represents a potential vulnerability.
Suppose a host is . . .

DNS Server: **No user accounts!!**



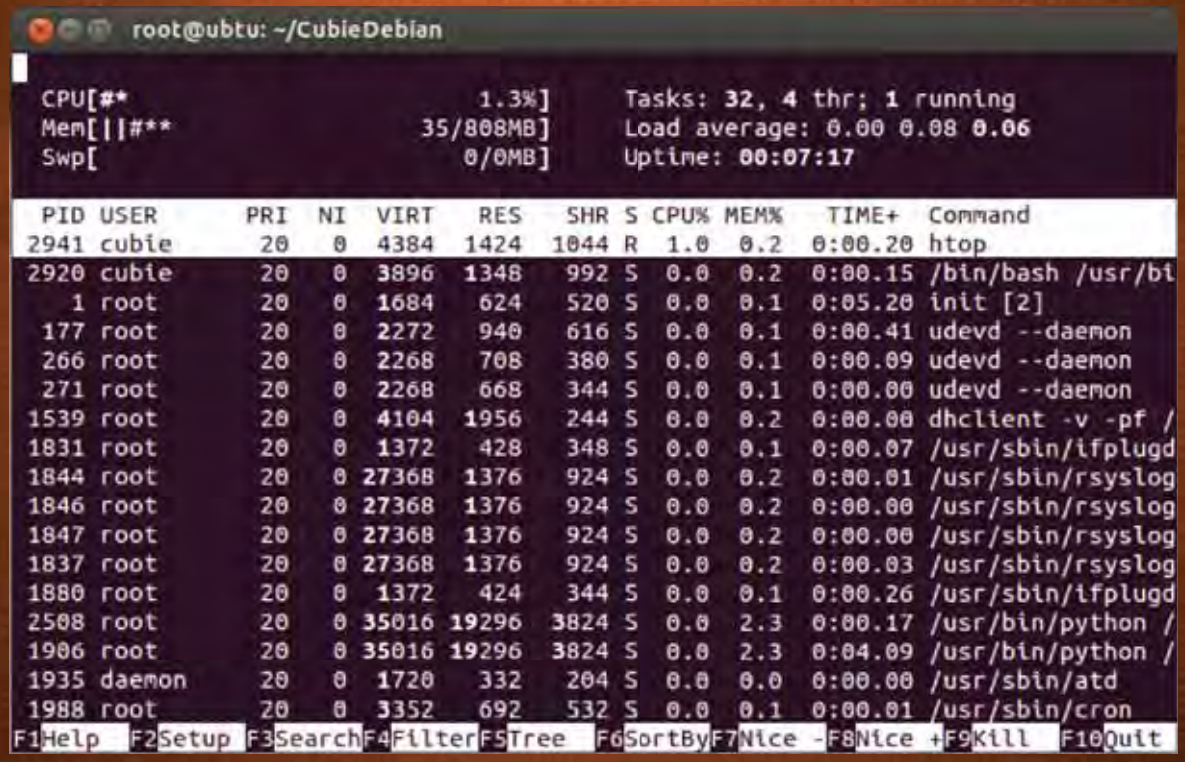
Or . . .

… *a scanning/multimedia host*: No web server on it!!

Module 3 – Countermeasures and Risk Management

Minimizing Processes with Elevated Privileges

Any process that runs as “root” or “Admin” is a potential avenue for *privilege escalation*



Sandboxing Servers

Sandboxing: running an application in a restricted environ so it has no access or resources other than what it needs to work

- Applications are often run "in a sandbox" during testing
- A server can be sandboxed to limit damage if compromised

Scenario: Suppose a web server is run under a dummy user account (e.g., *web*). What happens if the server is compromised? What access and privileges might the intruder get?

What if the web server was run under an administrator's account instead?

Separation of Duties

Different functions on a network are handled by different accounts, each with its own least-privilege access

- Helps prevent an adversary from escalating privileges
- Sensitive operations may be divided among privileged users to minimize the impact of a breach

Examples:

- Multiple keys for missile launches
- Database administrator has no general user privileges
- System Administrator role not permitted to perform system audits (ISSO role)

Module 3 – Countermeasures and Risk Management

Principle 3 – **Vigilance**

Every system should be continuously monitored, with an immediate and effective response to any signs of unexpected or unauthorized activity.

Questions?

Thanks for your time! ☺

rita.doerr@cyber.nsa.gov

Become a Cyber Warrior for Free Courtesy of Uncle Sam

Open-source tools and resources for enhanced Training and Simulation

CERT® Cyber Workforce Development

Chris May
18 Oct 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0578

Agenda

Introduction

Overview and Demos of Open-source Training Tools

- TopoMojo
- Crucible
- TopGen/GreyBox
- GHOSTS
- WELLE-D
- SCADASim
- FinSim
- Foundry Virtual Appliance
- President's Cup Cybersecurity Competition

Welcome and Logistics

Introductions:

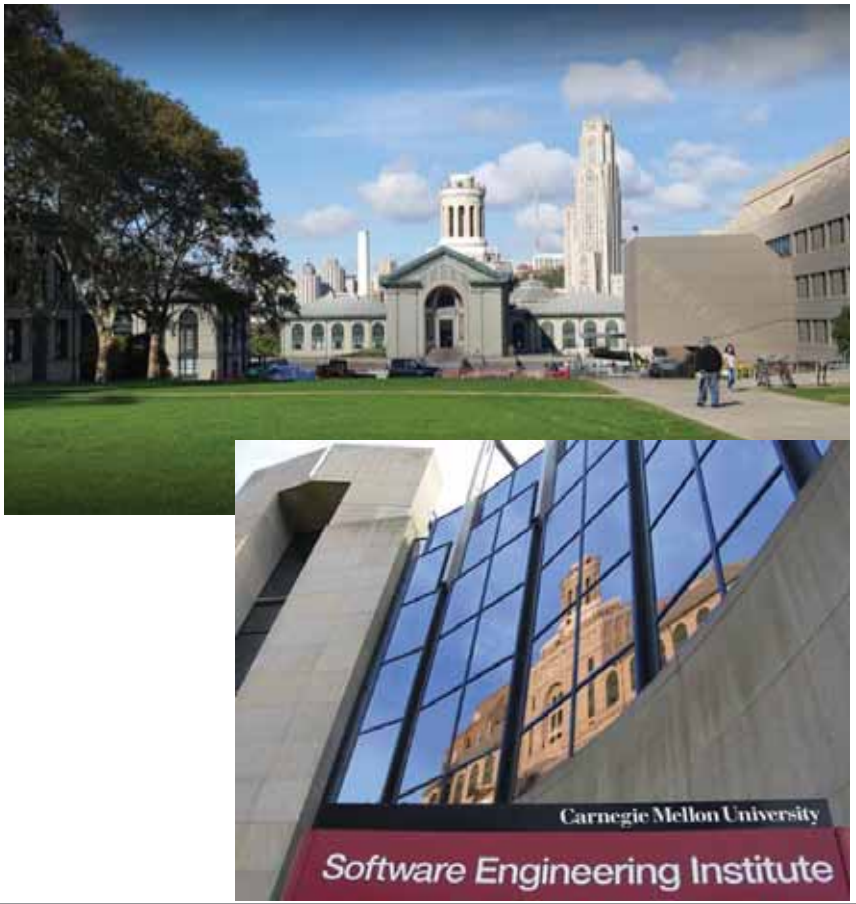
Chris May - CMU/SEI since 2001, IUP ‘92

Purpose:

- Build awareness of CMU/SEI’s open-source software developed to enhance cybersecurity training and simulations
- Encourage interaction and dialogue on emerging cybersecurity training and simulation requirements and best practices

Challenge:

Try out some of the technical challenges we created for the President’s Cup Cybersecurity Competition



Cybersecurity Professionals Need Practice!

Cyber Ranges (sandboxes) and Simulators let you:

TopoMojo

Simple Lab Builder and Player

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Motivation

Make it easy and convenient for users to create, share, and consume hands-on training

- 100% browser-based

Essential for building real-world skills and experience – especially in the cyber domain

- Lots of Cyber Gurus out there, need tool to share their expertise with others

Enable large-scale cybersecurity competitions

TopoMojo Features

Lab Builder

Lab Player

Competition Engine

Collaboration

File upload

Document editor

Resource limits

Management Dashboard

TopoMojo

DEMO

Crucible

Cyber Range (sandbox)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Crucible Simulation Framework (a.k.a. **Cyber Range**)

- Application framework for cyber modeling and simulation.
- Enterprise-grade tools to design, deploy, and manage training labs and exercises, both facilitated and on-demand.

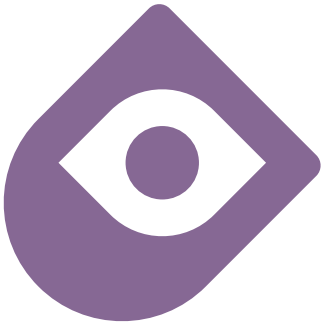
Crucible Core Components

Player

Caster

Steamfitter

Alloy



SEER

Crucible

DEMO

TopGen and Greybox

Internet Simulation Tools

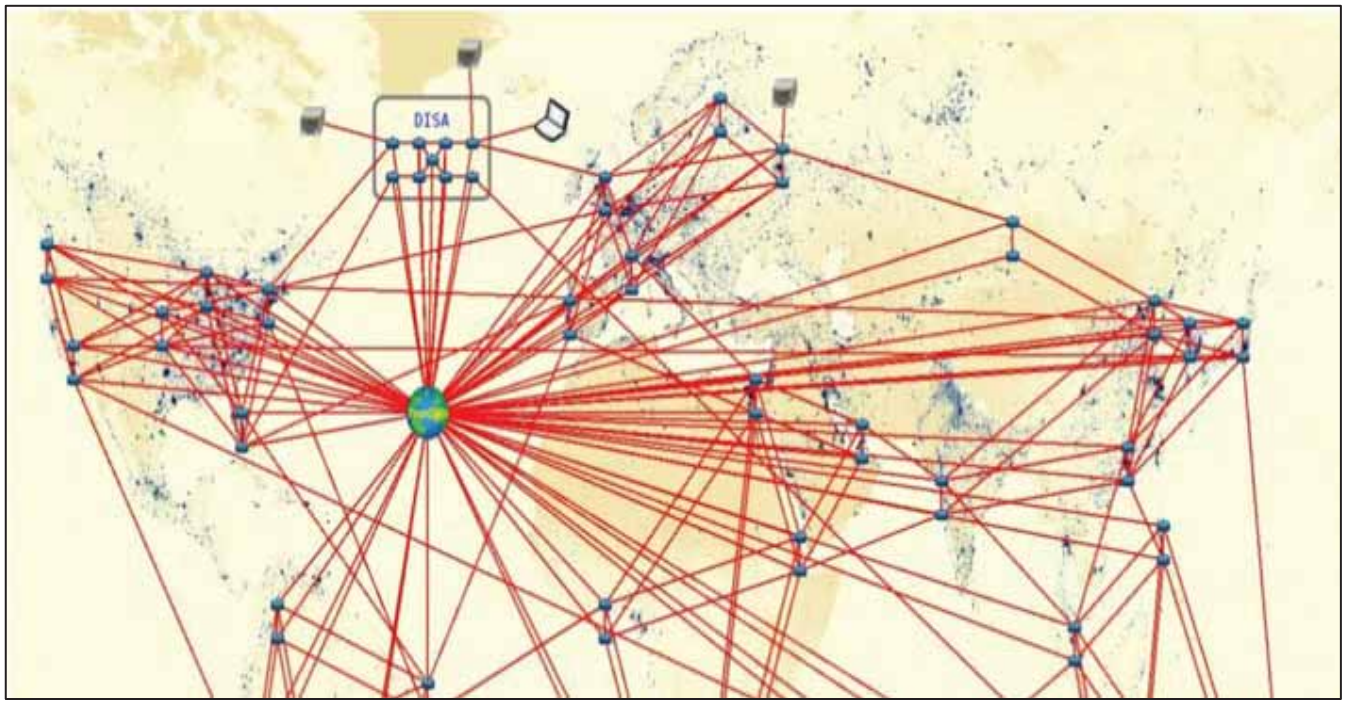
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

TopGen & GreyBox

Designed to bring Internet Services to ‘Air-Gapped’ networks

Application Virtualization via containers

Portable and Extensible (1 VM)



TopGen / Greybox Features

TopGen

- WWW (http and https)
  - Scrape live sites with wget script
- DNS
- Email
- Tor
- Bitcoin

Greybox (Internet in a box)

- Leverages the CORE open-source network simulator
- 70+ routers (containers) running BGP
- All TopGen services running

TopGen and Greybox

DEMO

GHOSTS in the Machine

Orchestrating Non-Player Characters (NPC) for a Realistic Cybersecurity Exercise Battlefield

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

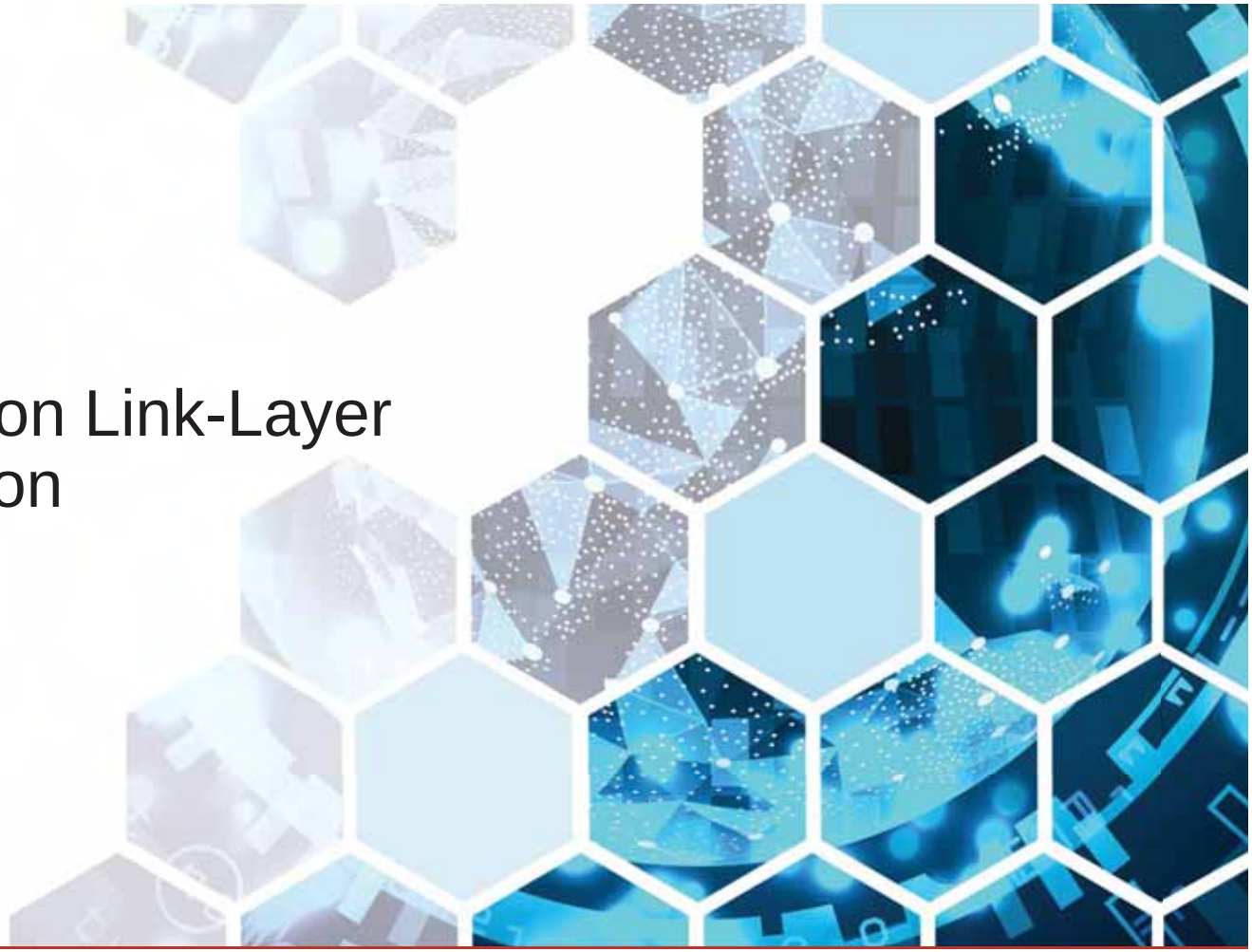
GHOSTS orchestrates realistic NPCs that:

- Are behaviorally accurate, fully-autonomous & represent an infinite array of possible interactions
  (from harmless administrators to hostile nation-state attackers)
- Match training realism with high training value
- Prepare effective cyber warfare teams for success in real-world situations

GHOSTS NPC Orchestration

DEMO

WELLE-D
Wireless Emulation Link-Layer Exchange Daemon



Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

WELLE-D
Wireless Emulation Link-Layer Exchange Daemon

Leverages frames from mac80211_hwsim driver

Uses VSOCK to transfer frames

Simulates wireless medium

Provides GPS simulation

Enables high-fidelity use of full-featured operating systems

WELLE-D

DEMO

SCADASim & FinSim

Industrial Control System and Banking Simulators

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

SCADASim – Features

Configurable PLCs

Modbus communications with HMIs

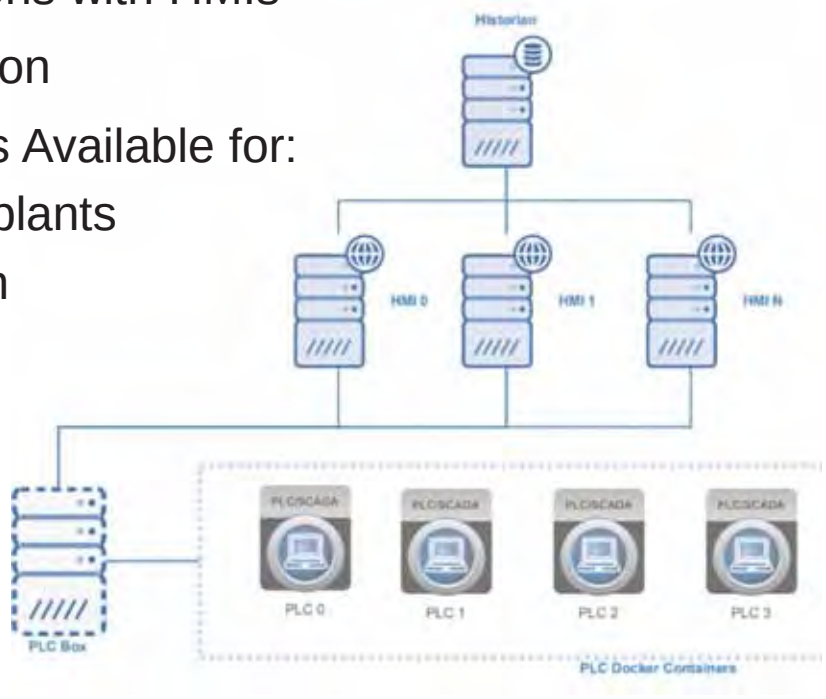
RapidSCADA integration

Sample Configurations Available for:

- Water treatment plants
- Power generation
- HVAC

Underlying technology

- Docker
- Postgres
- JSON



SCADASim

DEMO

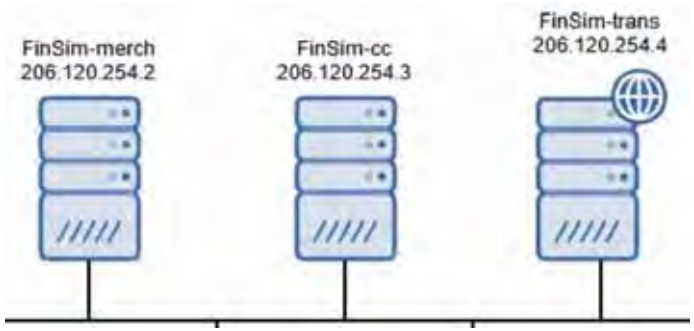
FinSim – Features

Model financial system within a training environment

- Banks (accounts and web interface)
- Credit Card processors
- Merchants

Underlying technology

- Python
- Angular
- Flask
- MySQL
- JSON Web Tokens (JWT)



FinSim

DEMO

Foundry Virtual Appliance

Ubuntu virtual machine

Docker and Kubernetes

TopoMojo

Gameboard

PostgreSQL Database

Use Case: CISA President's Cup

- Presidential Executive Order 13870
- Cyber competition among DoD and federal executive workforce solving challenges
- 1,000s of individual and team participants
- Integrate immersive (gamified) experiences
- Platform and challenges released as open-source

https://presidentscup.cisa.gov/

Resources and Contact Info

https://sei.cmu.edu/go/cwd-tools	https://github.com/cmu-sei/**vtunnel**
https://github.com/cmu-sei/**crucible**	https://github.com/cmu-sei/**welled**
https://github.com/cmu-sei/**TopoMojo**	https://github.com/cmu-sei/**SCADASim**
https://github.com/cmu-sei/**topgen**	https://github.com/cmu-sei/**finsim**
https://github.com/cmu-sei/**greybox**	https://github.com/cmu-sei/**foundry-appliance**
https://github.com/cmu-sei/**GHOSTS**	https://github.com/cmu-sei/**Crucible.Appliance**

Chris May: cjm@cert.org
info@sei.cmu.edu

Challenge Time!

https://iupsec.cmusei.dev/

Questions ?

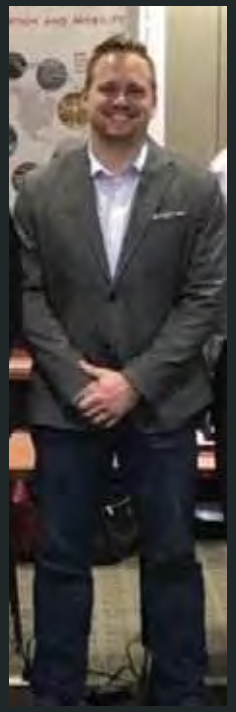
Designing Systems for Security:

Walls are Only as Secure as They are Designed

Nigel Wright
October 18, 2022
2022 IUP CyberSecurity Day

Today's Agenda

- Introduction
- System Design
  - What is a System
  - Allocation of System Features
- Design of Interfaces Elements
- Evaluating Tradeoffs
- Tools for Trade Off Consideration
- ABT - Always Be Testing
- Case Studies of Poor System Design



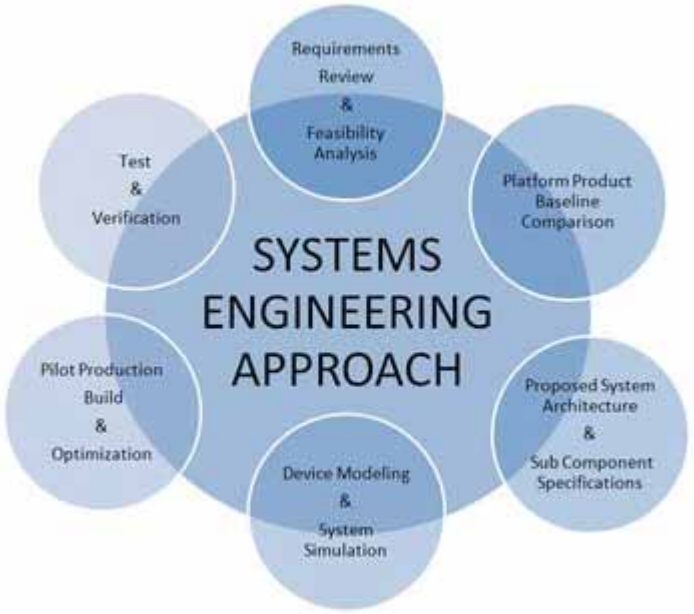
Hello!

About Nigel!

- **Pittsburgher**
  Grew up south of Pittsburgh in California, PA.
- **Developing Safety Critical Autonomous Systems!**
  Defense, Medical Automated Rail Signaling Transit, RoboTaxi's and Human Lead Autonomous Trucks

Systems Design & CyberSecurity

Approach to holistic look at development to ensure that the system (hardware and software) are free of vulnerabilities

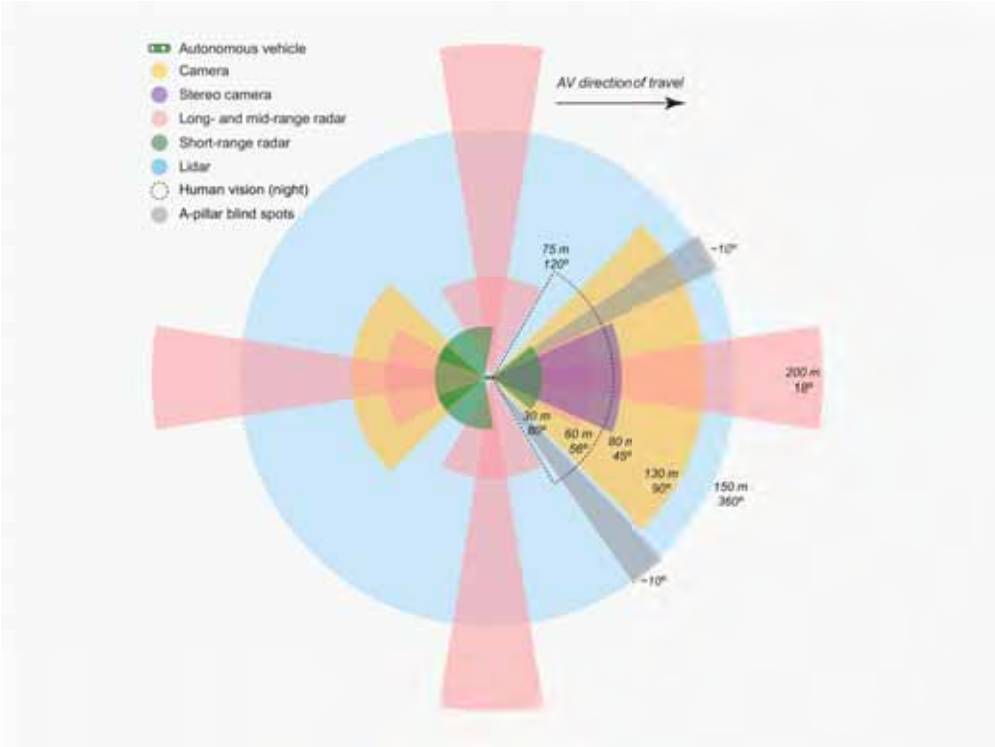


What is “Systems” Engineering

Systems engineering is an **interdisciplinary** field of engineering and engineering management that focuses on how to design and manage complex systems over their life cycles.

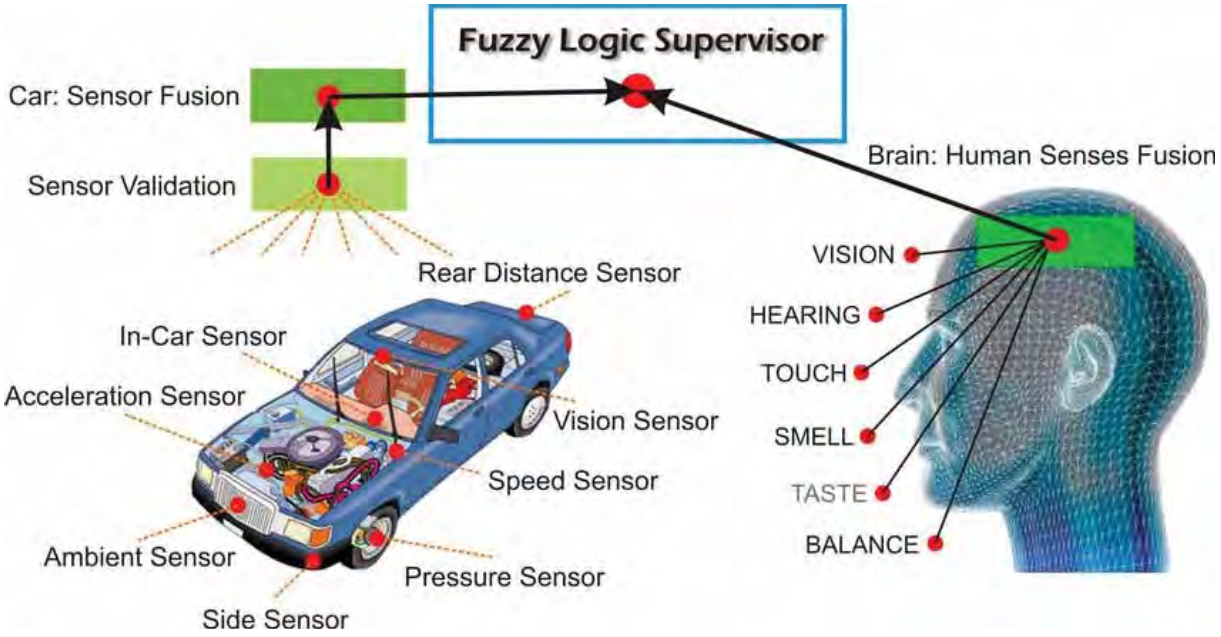
This includes, software, hardware, cyber-security, communications, supply chain…

Applying “Systems” Understanding to specific contexts



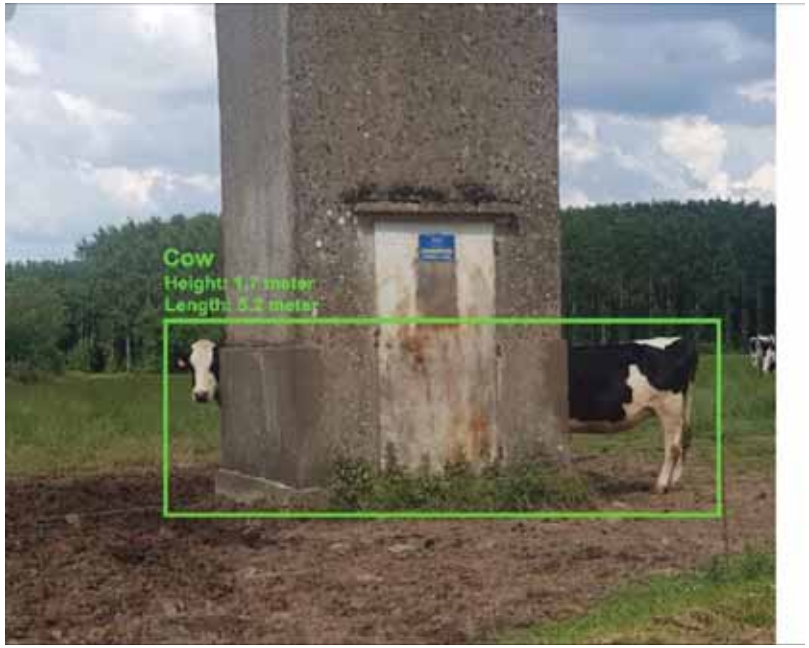
Example of a “generic autonomous vehicle sensor coverage overlay, color coded by sensor type.

Applying “Systems” Understanding to specific contexts



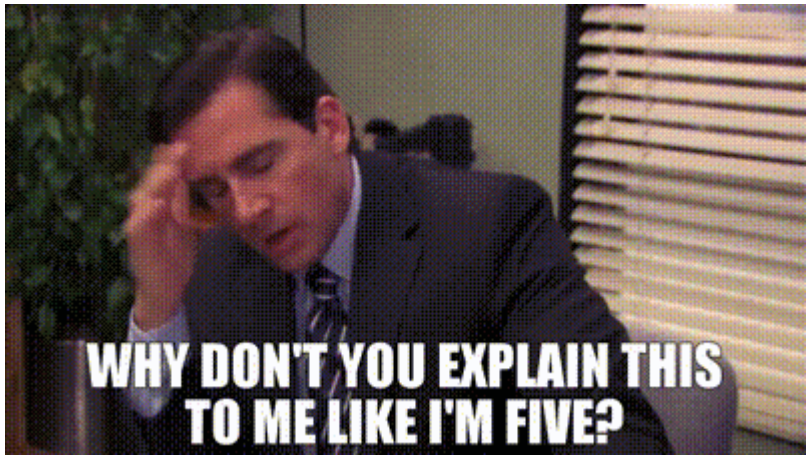
Sensing, and “computing” systems of a driving task

Applying “Systems” Understanding to specific contexts

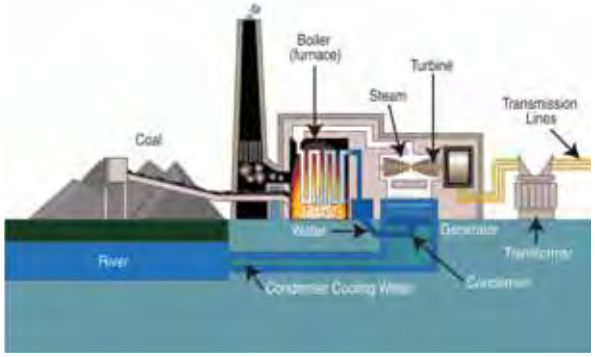


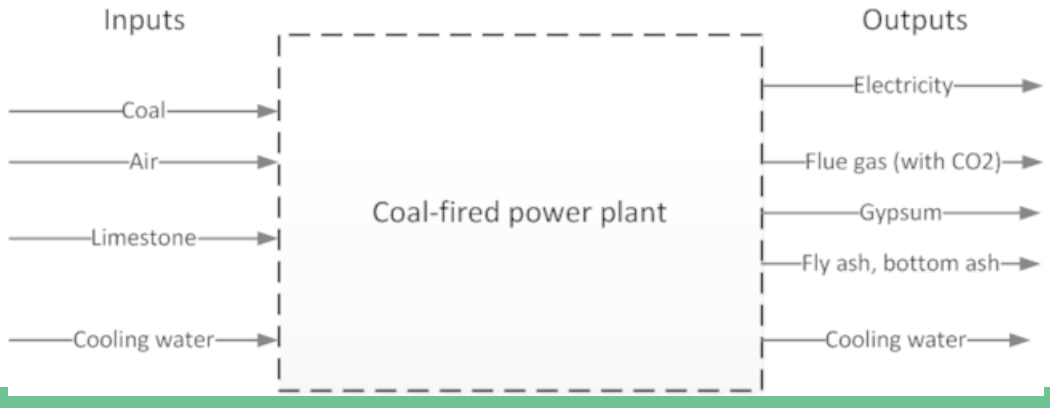
Example of a AI Detection

Using Systems Engineering to “Simplify” Understandings



Decomposing into a System Diagram



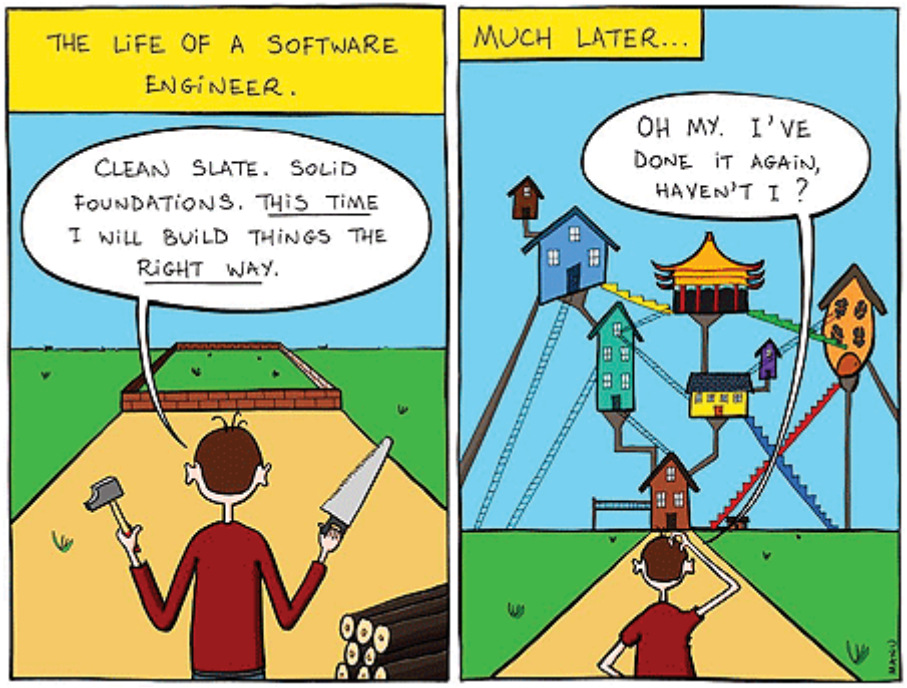


Systems Engineering methodologies enable architectural design

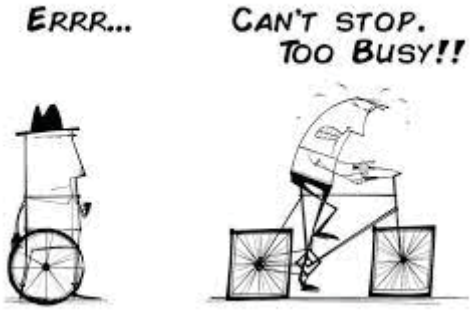
Systems Engineering methodologies enable designers to architectural decisions that support;

- security (data encapsulation)
- robustness (redundancy)
- abstraction (data exchange)

Systems Architecture



As engineers, you will need to be thoughtful about how the pieces of your systems interact…



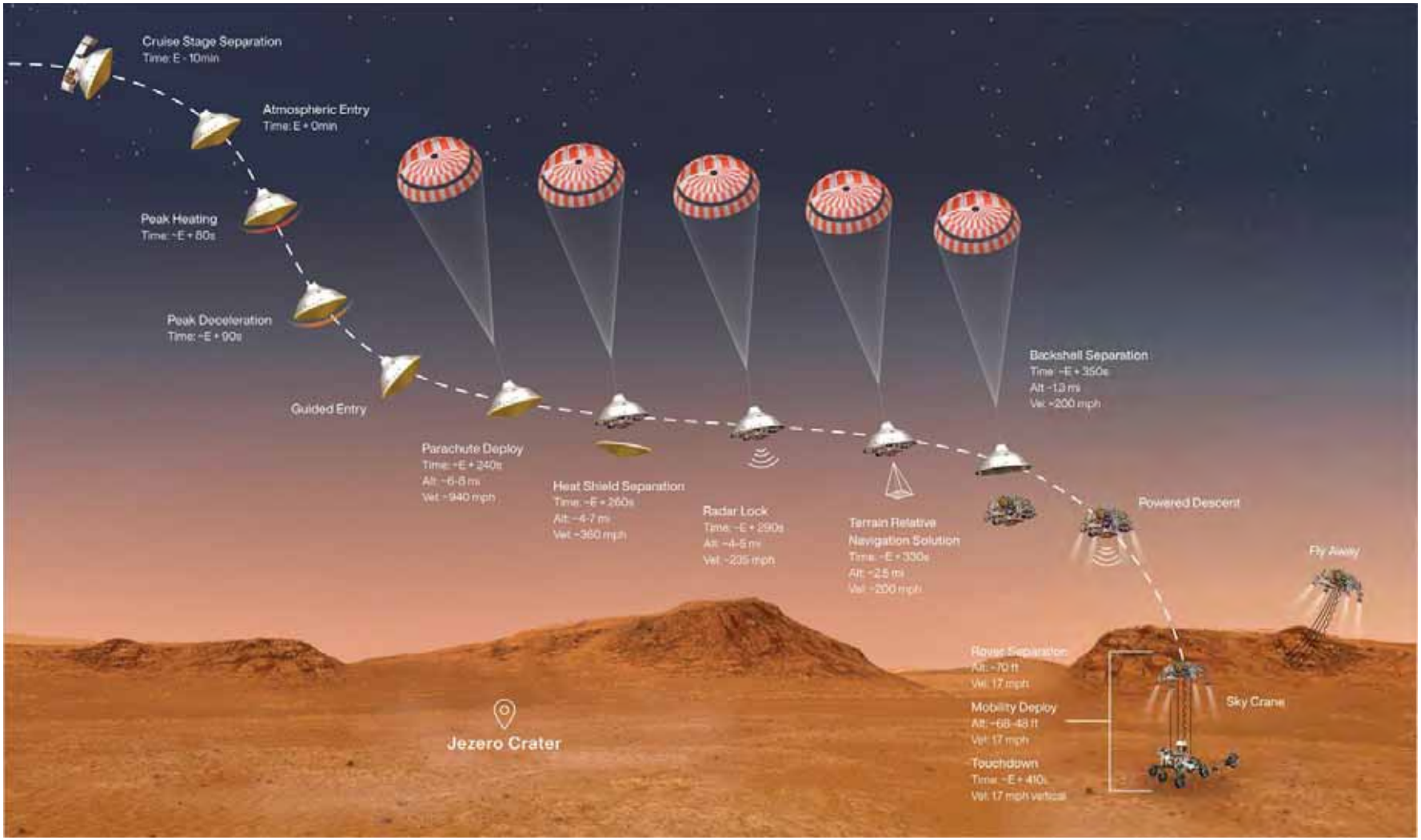
A “Secure” System

Everything is locked up tight!

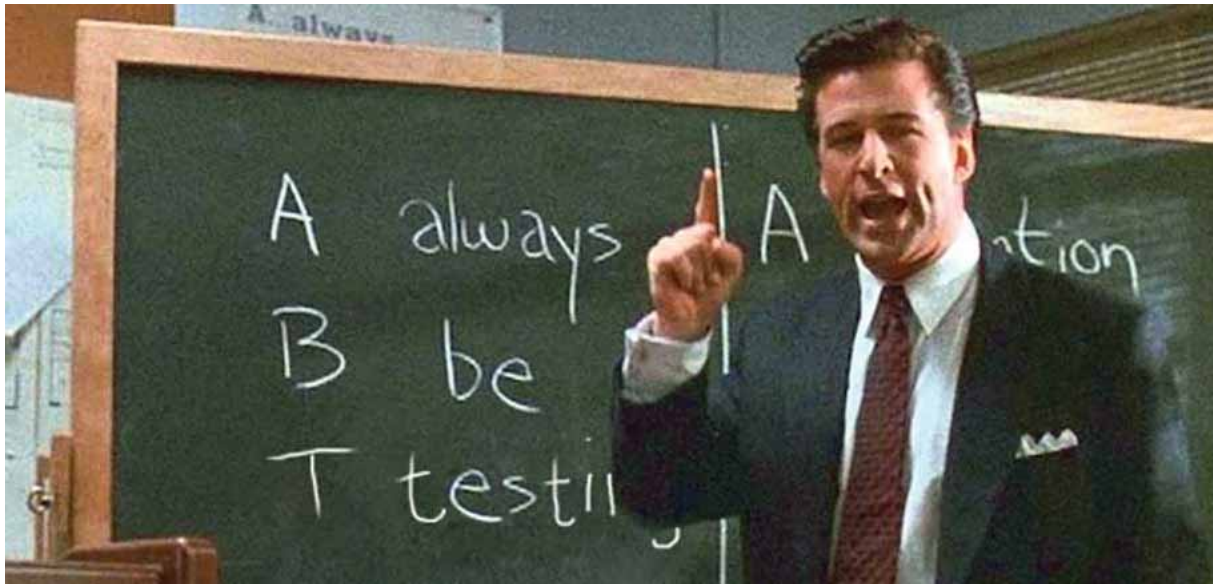
Toolkit - Concept of Operations

A “concept of operations” is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system.

This enables all parties to understand at a glance the way that a complex system is intended to behave.

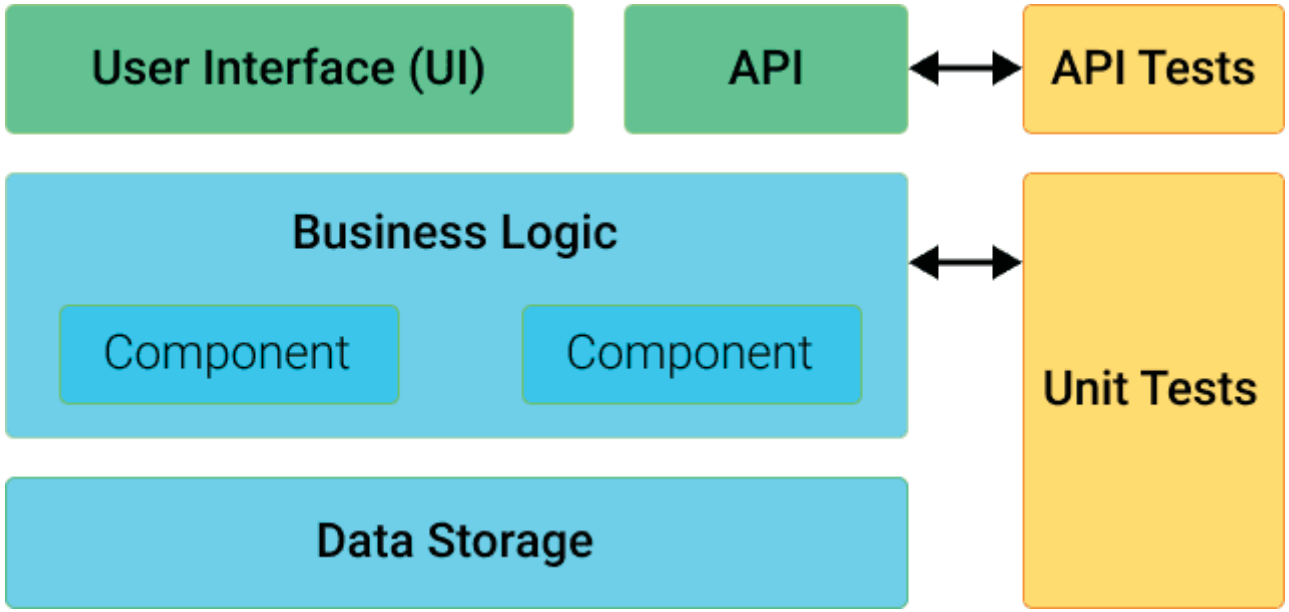

Cruise Stage Separation
Time: E - 10min
Atmospheric Entry
Time: E + 0min
Peak Heating
Time: ~E + 80s
Peak Deceleration
Time: ~E + 90s
Guided Entry
Parachute Deploy
Time: ~E + 240s
Alt: ~6-8 mi
Vel: ~940 mph
Heat Shield Separation
Time: ~E + 260s
Alt: ~4-7 mi
Vel: ~360 mph
Radar Lock
Time: ~E + 290s
Alt: ~4-5 mi
Vel: ~235 mph
Terrain Relative Navigation Solution
Time: ~E + 330s
Alt: ~2.5 mi
Vel: ~200 mph
Backshell Separation
Time: ~E + 350s
Alt: ~1.3 mi
Vel: ~200 mph
Powered Descent
Fly Away
Rover Separation
Alt: ~70 ft
Vel: 17 mph
Mobility Deploy
Alt: ~66-48 ft
Vel: 17 mph
Touchdown
Time: ~E + 410s
Vel: 17 mph vertical
Sky Crane
Jezero Crater

ABT - Always Be Testing



Glenn Gary Glenn Ross's famous scene of system validation

ABT - Always Be Testing - Examples



System Diagram of a Software Application

ABT - Always Be Testing - Examples

Function Testing

Bounds Checking for return values

Range Sweeping for incoming parameters

What happens if this function is passed a null pointer, an invalid parameter?

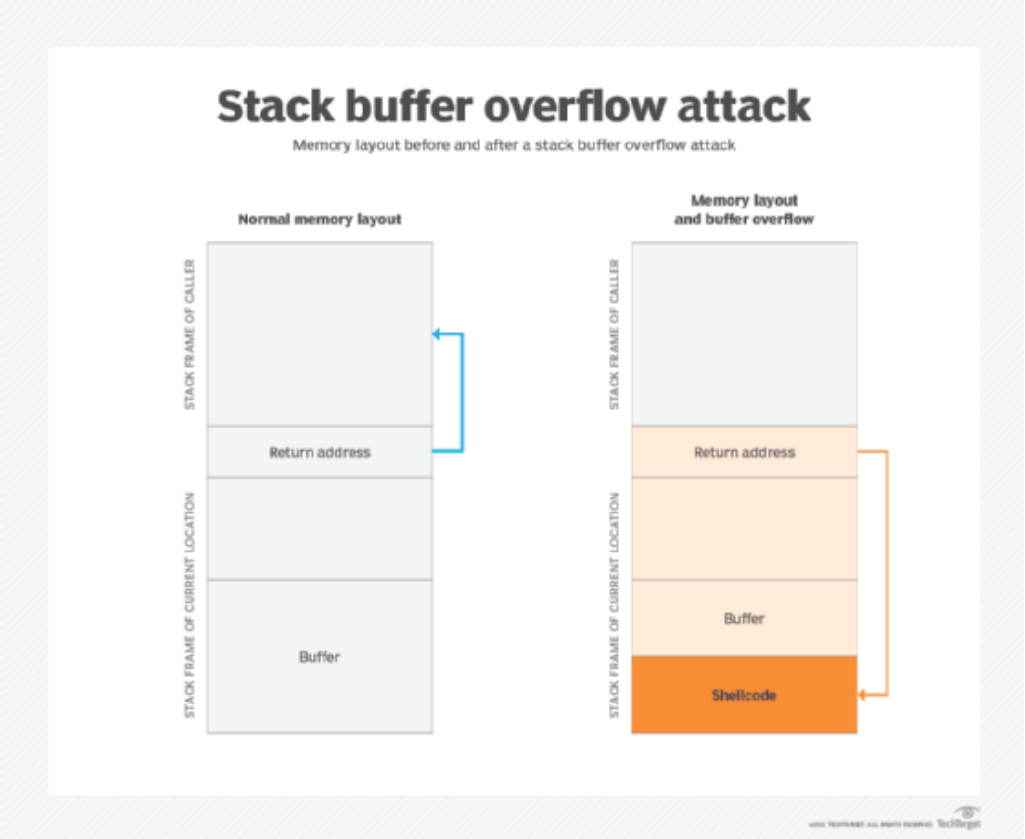
Are incoming parameters sanitized?

Can this function be overloaded?

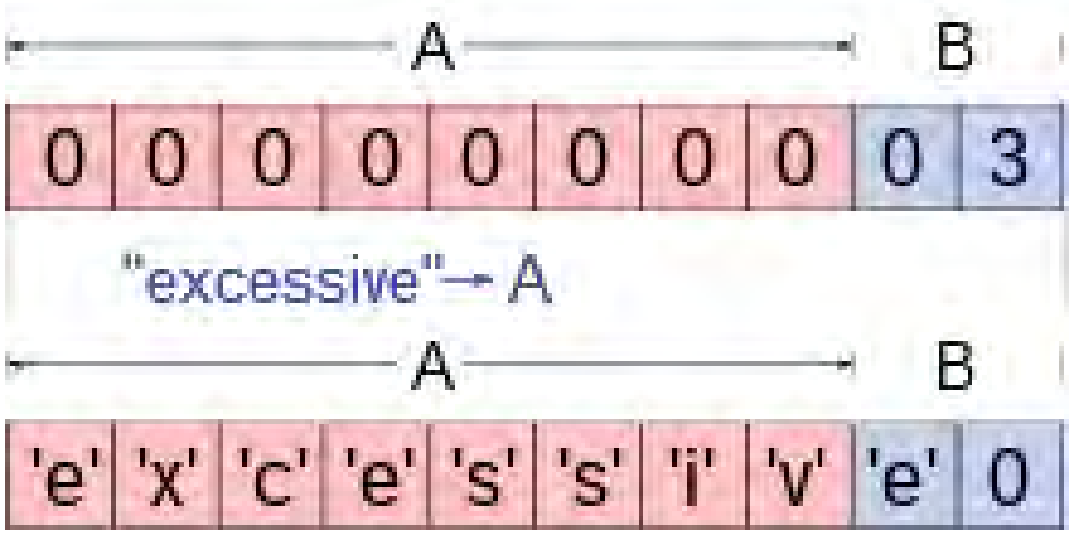
Buffer Overflow Examples

A buffer overflow occurs when a program is able to write more data to a buffer—or fixed-length block of computer memory—than it is designed to hold.

Then the excess data will overflow into the adjacent buffer, overwriting its contents and enabling the attacker to change the flow of the program and execute a code injection attack.

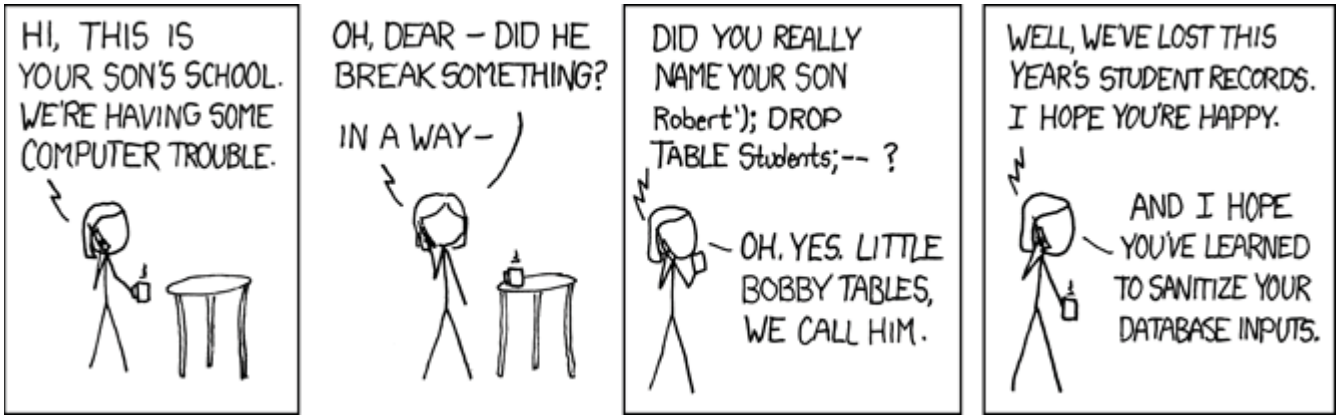


Buffer Overflow Examples

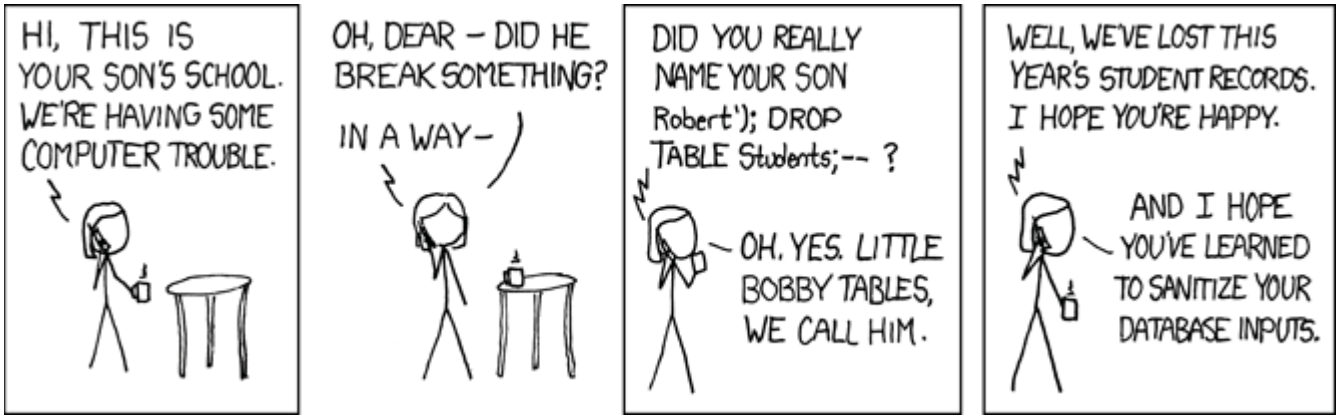


String "excessive" stepping into variable space for B

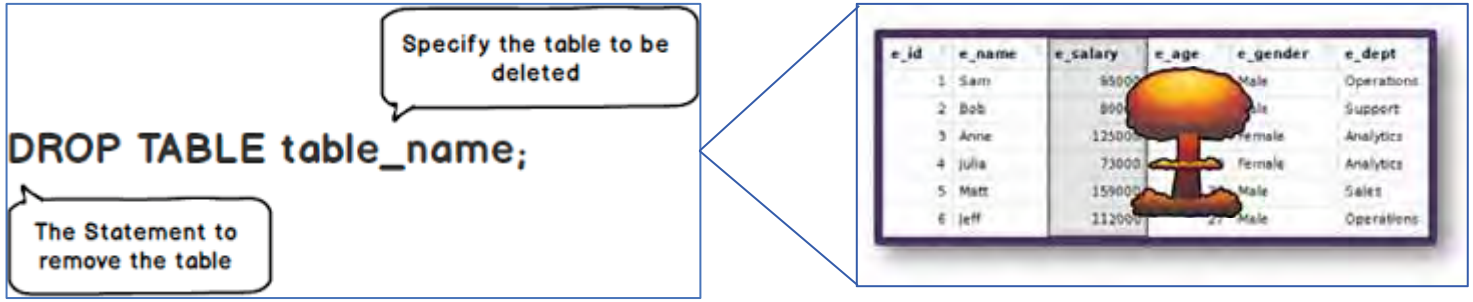
Example Sanitizing Inputs: Little Johnny Drop Tables



Example Sanitizing Inputs: Little Johnny Drop Tables

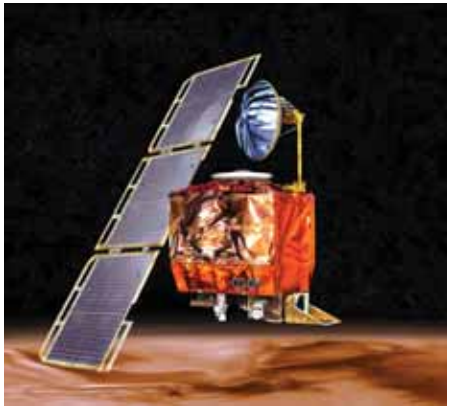


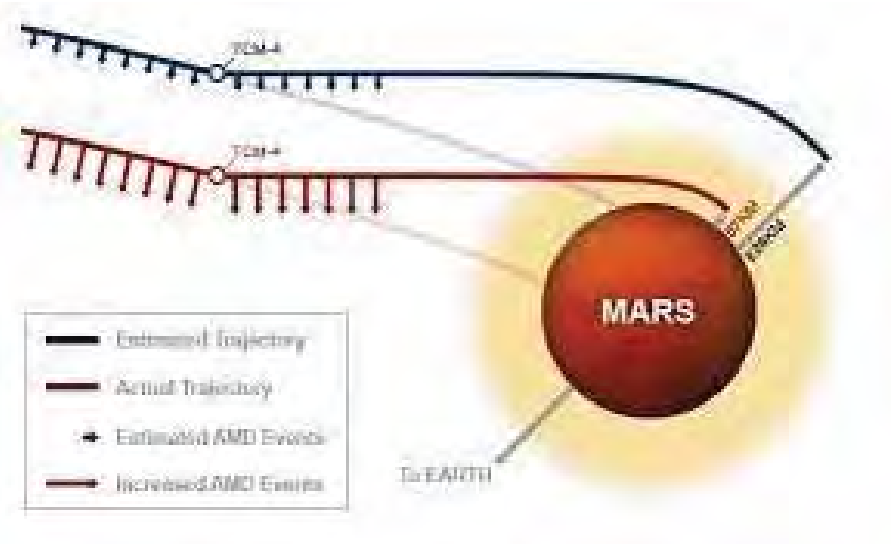
SQL Primer;



Integration Errors - Input Type Checking

1999, Nasa burnt up a $200 million dollar Mars Climate Orbiter when the engineers failed to realize one function was expecting units in **english**, the other in **metric…**





NASA Climate Orbiter

Integration Errors - Input Type Checking

Remember the Mars Climate Orbiter incident from 1999?

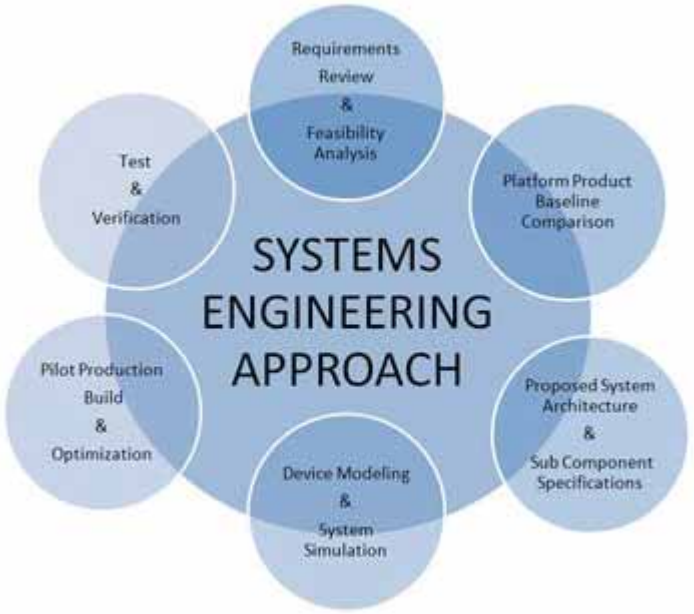
Closing Thoughts. . .

Ensure that you take a step back and think of the overall "system" and it's use…

Closing Thoughts. . .

Closing Thoughts. . .

Taking a structured, pragmatic approach enables rapid deployment… and ultimately enables a more robust, scalable and safe system…



Q&A

AFRL

Controlled by: AFRL/RI
CUI Category: N/A
Distribution/Dissemination Control: Distribution A
POC: B. Wysocki, AFRL

Understanding Information Warfare

2022 CYBER SECURITY DAY

Indiana University of Pennsylvania

Dr. Bryant Wysocki
DAF Technical Advisor

Information Warfare is everywhere and growing

Information Warfare is **any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions**; protecting ourselves against those actions and exploiting our own military information functions. (Air University)

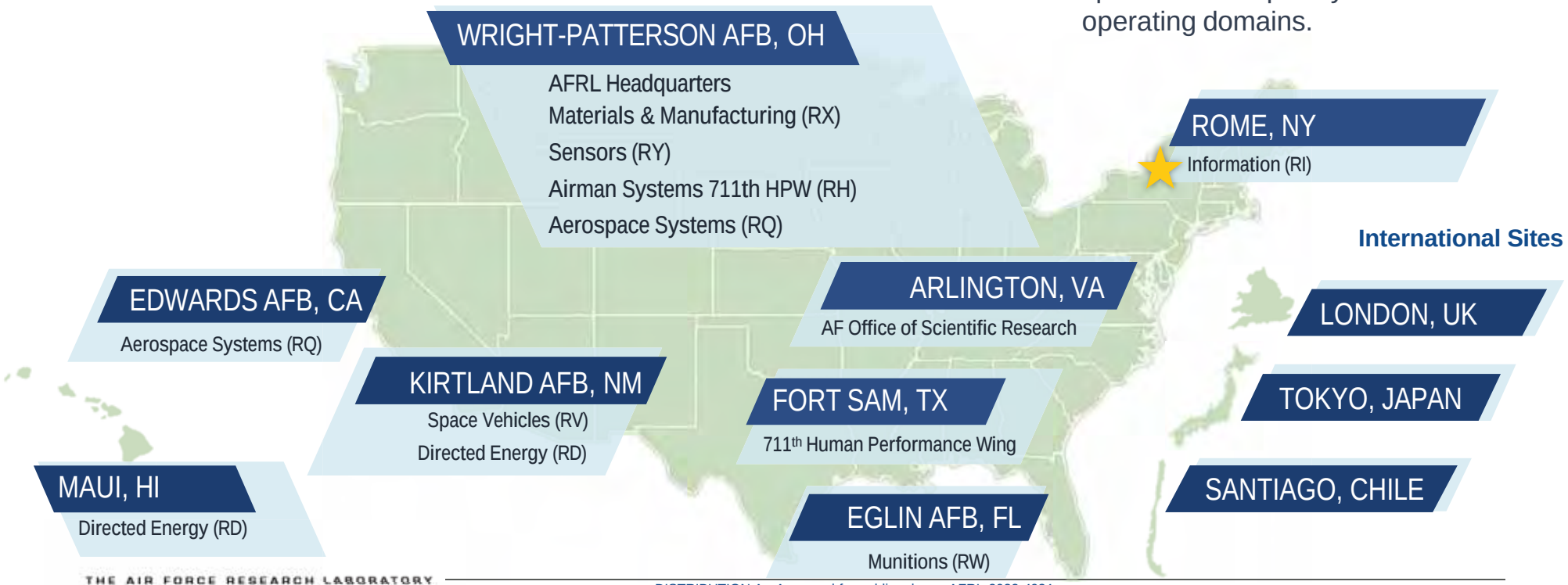
Information warfare is an operation conducted in order to gain an information advantage over the opponent. (NATO paper on disinformation)

Information warfare is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest but in the interest of the one conducting information warfare. (Wikipedia)

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

MISSION: We lead, discover, develop and deliver science, technology and innovation for Warfighters.

VISION: To arm Warfighters that dominate in time, space and complexity across all operating domains.



WRIGHT-PATTERSON AFB, OH
AFRL Headquarters
Materials & Manufacturing (RX)
Sensors (RY)
Airman Systems 711th HPW (RH)
Aerospace Systems (RQ)

ROME, NY
Information (RI)

EDWARDS AFB, CA
Aerospace Systems (RQ)

ARLINGTON, VA
AF Office of Scientific Research

KIRTLAND AFB, NM
Space Vehicles (RV)
Directed Energy (RD)

FORT SAM, TX
711th Human Performance Wing

MAUI, HI
Directed Energy (RD)

EGLIN AFB, FL
Munitions (RW)

International Sites
- LONDON, UK
- TOKYO, JAPAN
- SANTIAGO, CHILE

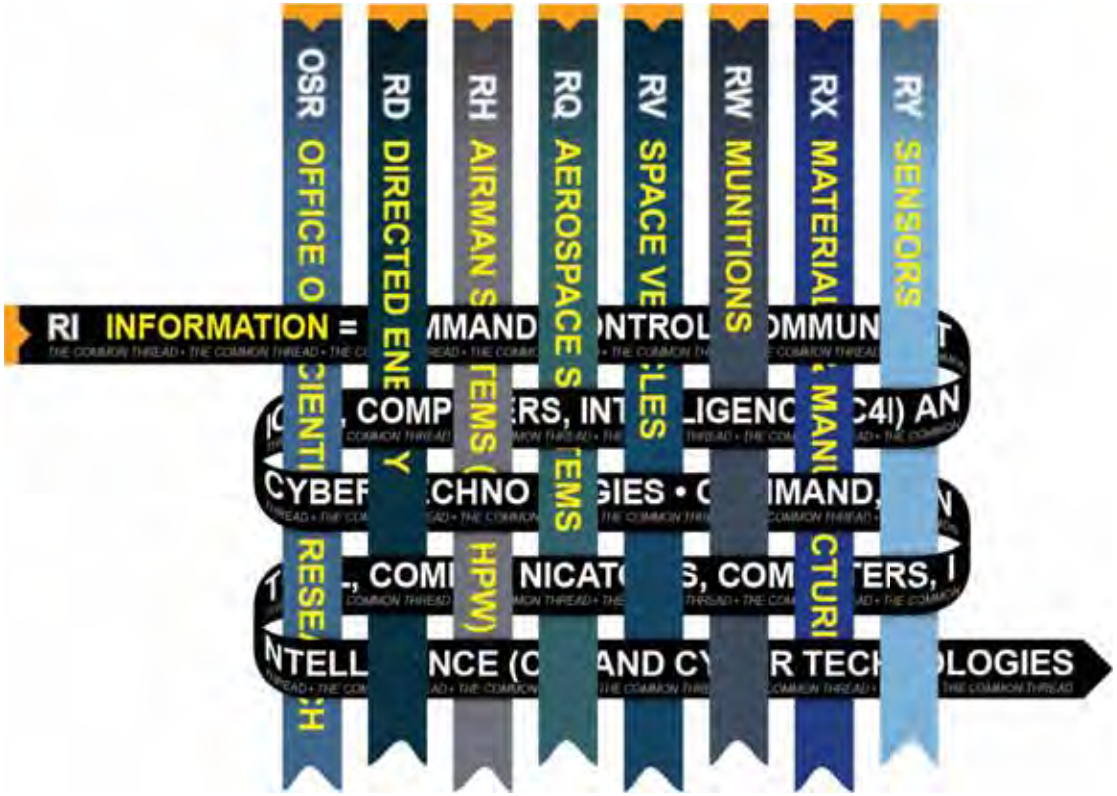
Information Directorate (RI)

MISSION:
To EXPLORE, PROTOTYPE, and DEMONSTRATE high-impact, game-changing technologies that enable the Air Force and Nation to maintain its superior technical advantage.

C4I&Cyber

VISION:
To LEAD the Air Force and Nation in COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE (C4I) AND CYBER science, technology, research and development.

Information Technologies Touch Every Core Mission



C⁴I&Cyber

Command, Control, Communications, Computers, Intelligence and Cyber

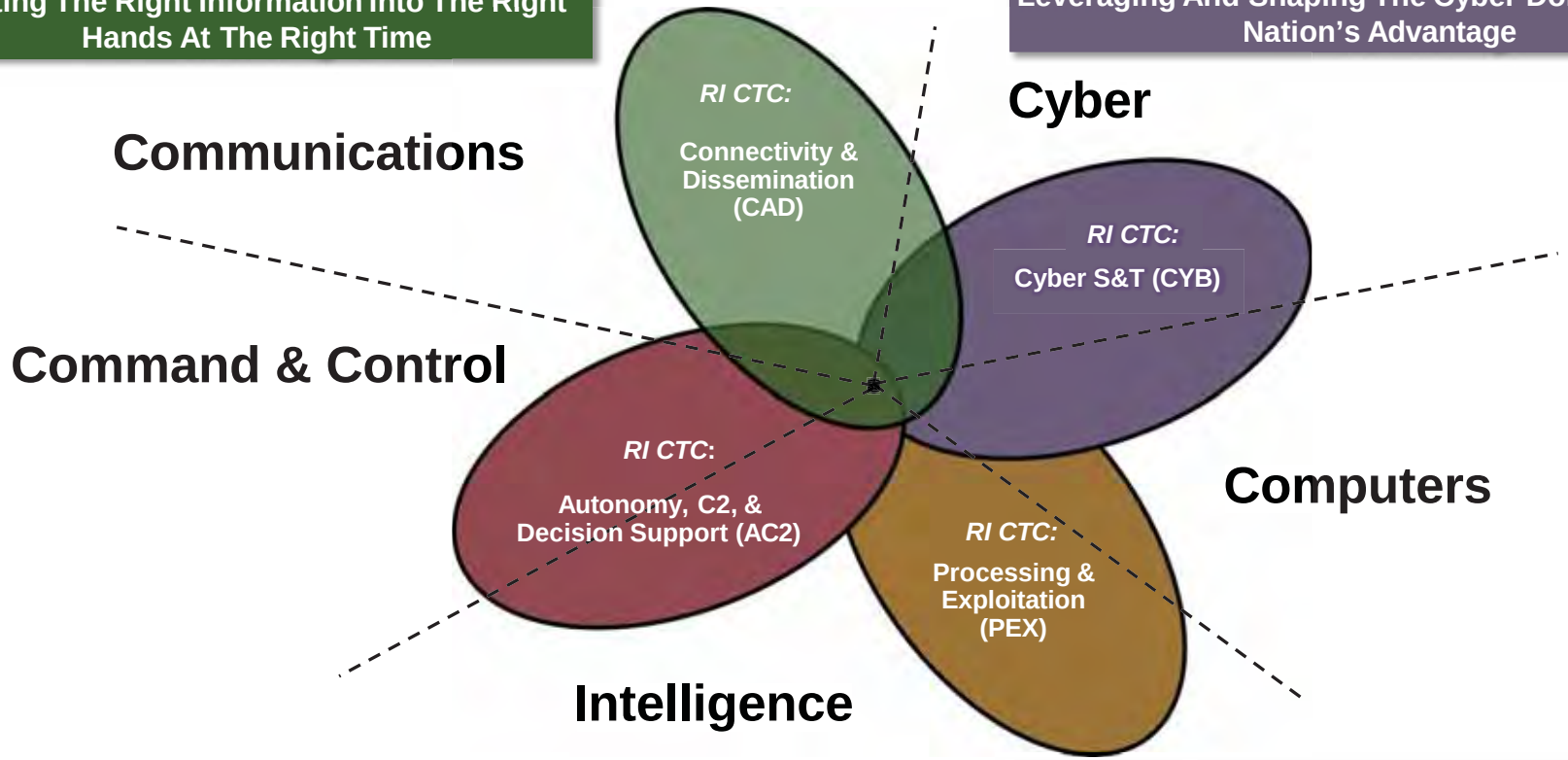
66% of RI programs are in collaboration with other AFRL TDs

- **16% Provide $**
- **52% SME Time**
- **32% $ + SME**

Information Directorate Core Technical Competencies (CTC)

Putting The Right Information Into The Right Hands At The Right Time

Leveraging And Shaping The Cyber Domain To The Nation's Advantage



Mastering Complexity of Multi-domain Command & Control

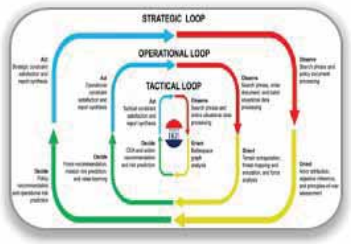
Exploiting Computing and Algorithms to Transform Big Data Into Information

AFRL Cross-Directorate Cyber Collaborations

RI	711HPW	RY	RV	RW
				
Mission Assurance Command & Control / Visualization Cyber Operations Communications & Networking Processing & Exploitation Signals Intelligence Electronic Protection	Cognitive Task Analyses Operator Selection & Training Adaptive Interfaces / Visualization	Electronic Warfare Avionics Protection	Space System Hardening	Munition Systems Cyber Resiliency

AFRL's Cyberspace Capability Leadership

Cyber S&T CTC Lines of Effort



Cyber Warfighting

Cyber warfighting technologies that support joint, integrated DCO-OCO-DODIN operations across all domains and levels of conflict. **Vision:** Cyber operations on par and integrated with air and space.

Cyber Assurance

Integrated components and processes that provide measureable and provable guarantees for current and future system architectures. **Vision:** Mission assurance in environments of heterogeneous trust.

EM-Cyber Convergence

Fusion of wired & wireless capabilities with advanced signal processing, enabling future integrated multi-domain ops and emerging missions. **Vision:** Cyber ops agnostic to medium and geography.

Information Warfare

Employment of Military Capabilities in and through the Information Environment

Threats in the News

BBC News 12.17.2018 *(Information Operations)*
Russia "meddled in all big social media" around US Election

CNN 12.3.2021 *(CyberOps/Exploitation)*
Suspected Chinese hackers breach more US defense and tech firms

ABC News 12.19.2020 *(CyberOps/Exploitation)*
Pretty clear "Russia behind SolarWinds hack, Pompeo Says, becoming 1st US official to blame Moscow

CNN 3.8.2022 (*Cyber Operations/Exploitation)*
Cybersecurity firm says Chinese hackers breached six US state agencies

Bloomberg Businessweek 12.21.2021
(CyberOps/Ransomeware)
The hackers who help keep Kim Jong Un in power (North Korea)

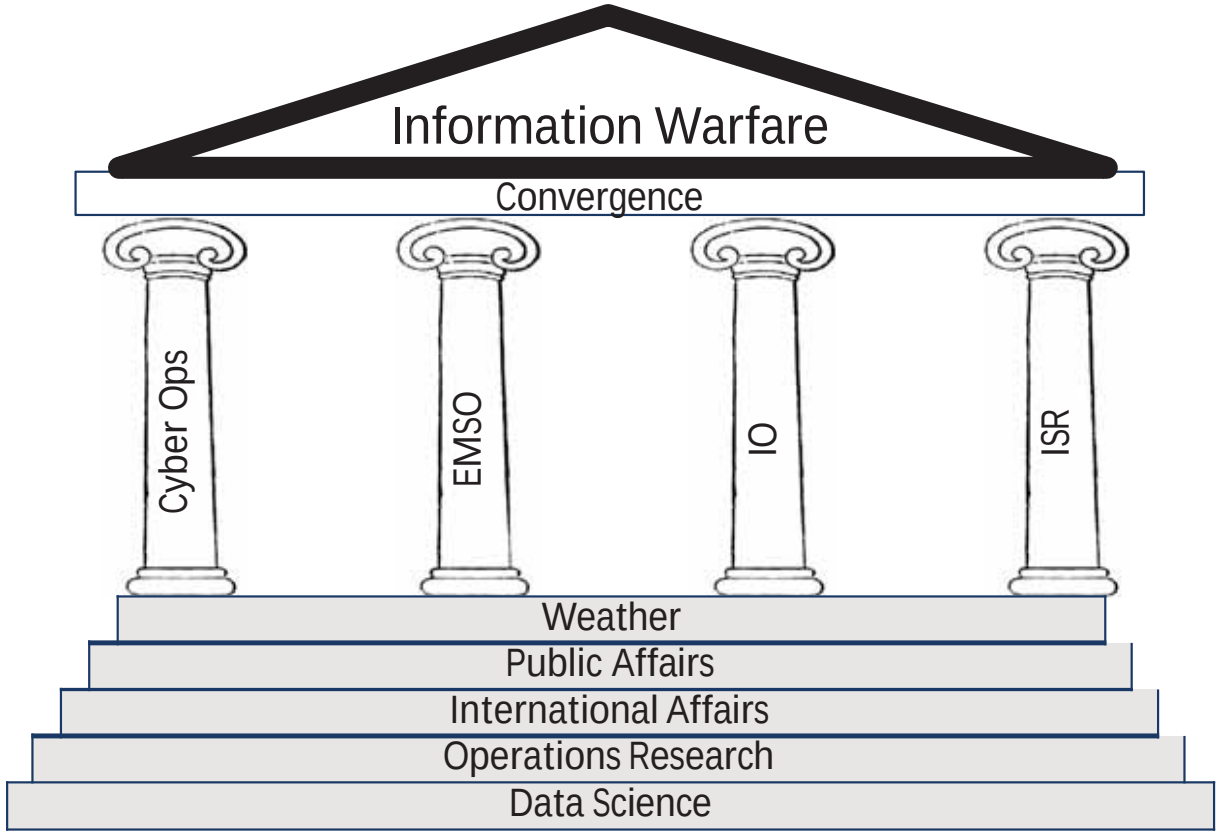
The CyberSecurity 202 – Analysis 2.7.2022 *(CyberOps/Exploitation)*
The News Corp breach illustrates how badly China wants to hack the U.S.

Science and Technology at-a-Glance

Major Themes	Consequences (for both defense and offense)	Effect on S&T Strategy
TIMELINES SHRINKING	• Cyber-speed decisions required at all levels • All domain is expanding to include new non-DOD entities and emerging IO tech • Contested	• Early and persistent engagement • Emphasize mission assurance • MVPs, DevSecOps, pipelines for S&T
COMPLEXITY INCREASING	• Multi-system-service-national-infrastructure • More interdependencies and data sharing • Cyber-attack consequences hard to predict • Beyond human capacity, AI assisted missions	• Emphasize minimalism and simplicity • Build systems that work in 'zero trust' • Take advantage of the complexity • End of sustainment -> continuous delivery
LANDSCAPES RAPIDLY CHANGING	• Constantly redefining battleground via new C4ISR technologies and applications, microelectronics, ML/AI, and Autonomy → New vulnerabilities surface all the time	• Budget is unstable and slow • Cyber cannot be an afterthought. • More coordination required everywhere • Volatility in S&T priorities and landscape
DOMAINS CONVERGING	• Rapid advance of effects • A platform's attack surface extends out through all its apertures • Single-domain stovepipes weaken impact	• Legacy and SOTA interoperability • Cyber cannot be an afterthought • Demands more coordination Labs/PEOs

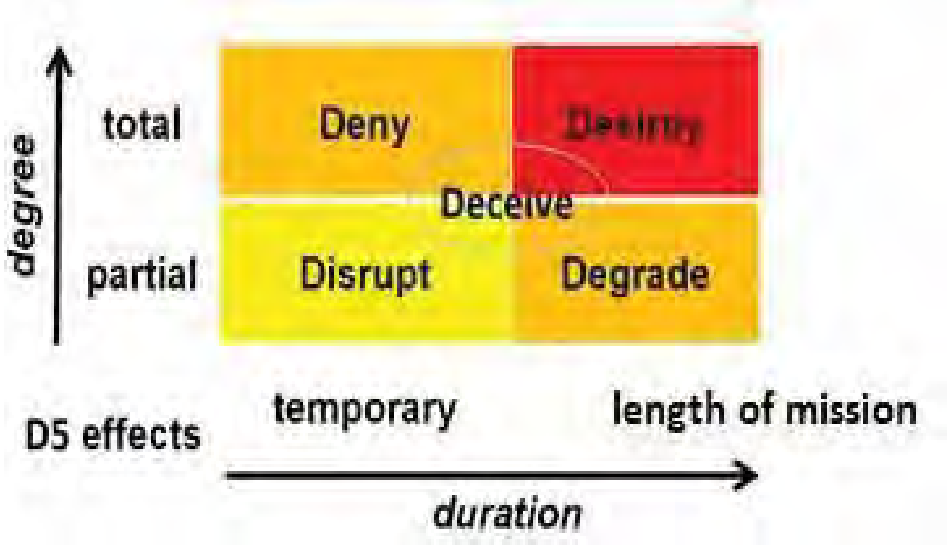
Science and Technology is a crucial enabler.

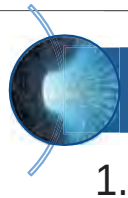
USAF Operating Concept for Information Warfare 30 Mar 2022



D5 Effects

- Specify the impact to compromised MEF in terms of disruption, degradation, denial, destruction based on degree and duration of effect
- The fifth D: deception, can achieve any of the other four D effects by convincing a user or system of the presence or absence of an effect.





Cyber Vulnerability Assessment

1. Identify the mission of the System Under Test (SUT).
2. List the Mission Essential Functions (MEF).
3. Map MEF cyber dependence along the six phases of the information lifecycle: generation, processing, storage, communication, consumption and destruction.
4. Draw an information boundary for the SUT.
5. Enumerate Information Exchange Requirements (IER) between the SUT and outside world.
6. Characterize each information flow across the information boundary
7. Estimate the mission impact of a compromise in the confidentiality, integrity or availability in each information flow.
8. Specify impact to compromised MEF as disruption, degradation, denial, destruction or deception.
9. Categorize vulnerability as architecture, specification or implementation.
10. Design cooperative tests to verify impact of information compromise.

In the fight

U.S. Army Cyber Command

How can you help?

Be Aware AND minimize your digital footprint

Digital Exhaust: What Everyone should know about Big Data, Digitization and Digitally Driven Innovation by Dale Neef

Be Informed about how your information can be used

The Social Dilemma – Documentary on NETFLIX

Be a discerning consumer of information

Influencing your perceptions

Get involved, we can use your help!

Come Join us at AFRL! afresearchlab.com

INFORMATION DIRECTORATE: C4I&Cyber

Global Persistent Awareness

Resilient Information Sharing

Rapid, Effective Decision-Making

Complexity, Unpredictability, and Mass

Speed and Reach of Disruption and Lethality

Questions

Image Reference slide

- Slide 2 - IW

Image on left Cyber Warrior: "Cyberwarfare and information warfare…" c4ISRnet.com, 4.25.2017
Image on upper right: "Information Warfare – Modern Diplomacy" moderndiplomacy.eu 3.7.2018
Image on lower right: "Information Warfare in 2021 – Are you protected from cyber attacks? – Connected IT Blog - Community.connection.com 19 Feb 2021

- Slide 3 - IW Global Power Competition Image of Chinese Flag – upload.Wikimedia.org/Wikipedia/commons

Image of Russian Flag – upload.Wikimedia.org/Wikipedia/commons

- Slide 4 - Threats in the News

Image upper left: BBC News – "Russia meddled in all big social media around us Election" - 12.17.2018
Image upper center: The Daily Beast – "China reveals its Cyberwar Secrets" - 4.14.2017
Image upper right: ABC news – "Pretty clear Russia behind Solar Winds …" - 12.19.2020
Image lower left: South China Morning Post scmp.com - 8.19.2020
Image lower center: Vox.com "How North Korea stole 235 gigabytes of classified US and South Korean military plans" – 10.13.2017
Image lower right: China's next generation of hackers techcrunch.com - 11.12.2021

- Slide 5 - USAF OC for IW

Image created by Scott Shyne (AFRL/RIG) 4.12.2022

- Slide 6 - In the fight -

Images: all official logos of USCYBERCOMMAND and their respective service commands

- Slide 7 - How can you help?

Image upper left: Wellframe.com/industry-insights "Harness your digital exhaust"
Image upper right: humanetech.com "The Social Dilemma"
Image lower left: news.standford.edu "The best way to counter fake news is…" 10.25.2021
Image lower right: project-manus.mit.edu/monthlychallenge277-2776493 "we-want-you-uncle-sam-we–want-you"