CySER Summer Workshop

Perspectives on Cyber

Sonja Glumich

Air Force Research Laboratory Information Directorate
VICEROY Air Force Program Manager

Disclaimer

Any opinions, findings, and conclusions or recommendations expressed in this presentation are those of the authors and do not necessarily reflect the views of the U.S. Air Force Research Laboratory, United States Air Force, Department of Defense, or the United States Government.

Approved for Public Release; Distribution Unlimited:
Case Number AFRL-2023-1578

About Me

- Worked for the Air Force Research Laboratory for 17 years
- Research Interests
  - Systems Engineering
  - Cyber Vulnerability Assessment
  - Cyber Education and Workforce Development
- Current VICEROY AF PM

Agenda

Presentation in three parts:

- Touch on Concepts from Joint and Air Force Cyber Doctrine
- Discuss the Challenges of Cyber
- Introduce VICEROY MAVEN

Cyber Doctrine

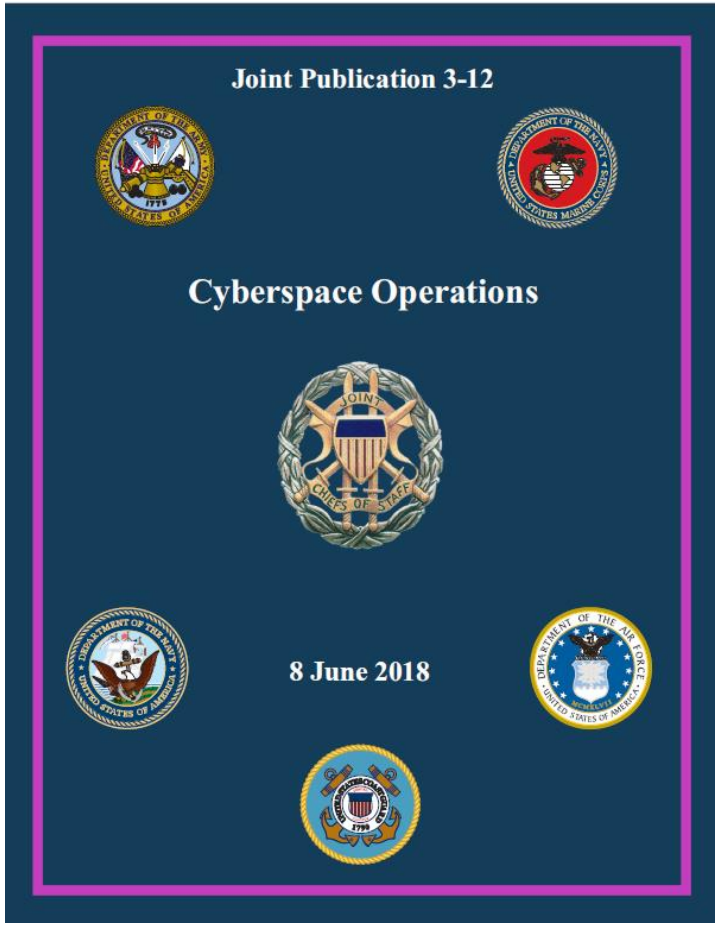
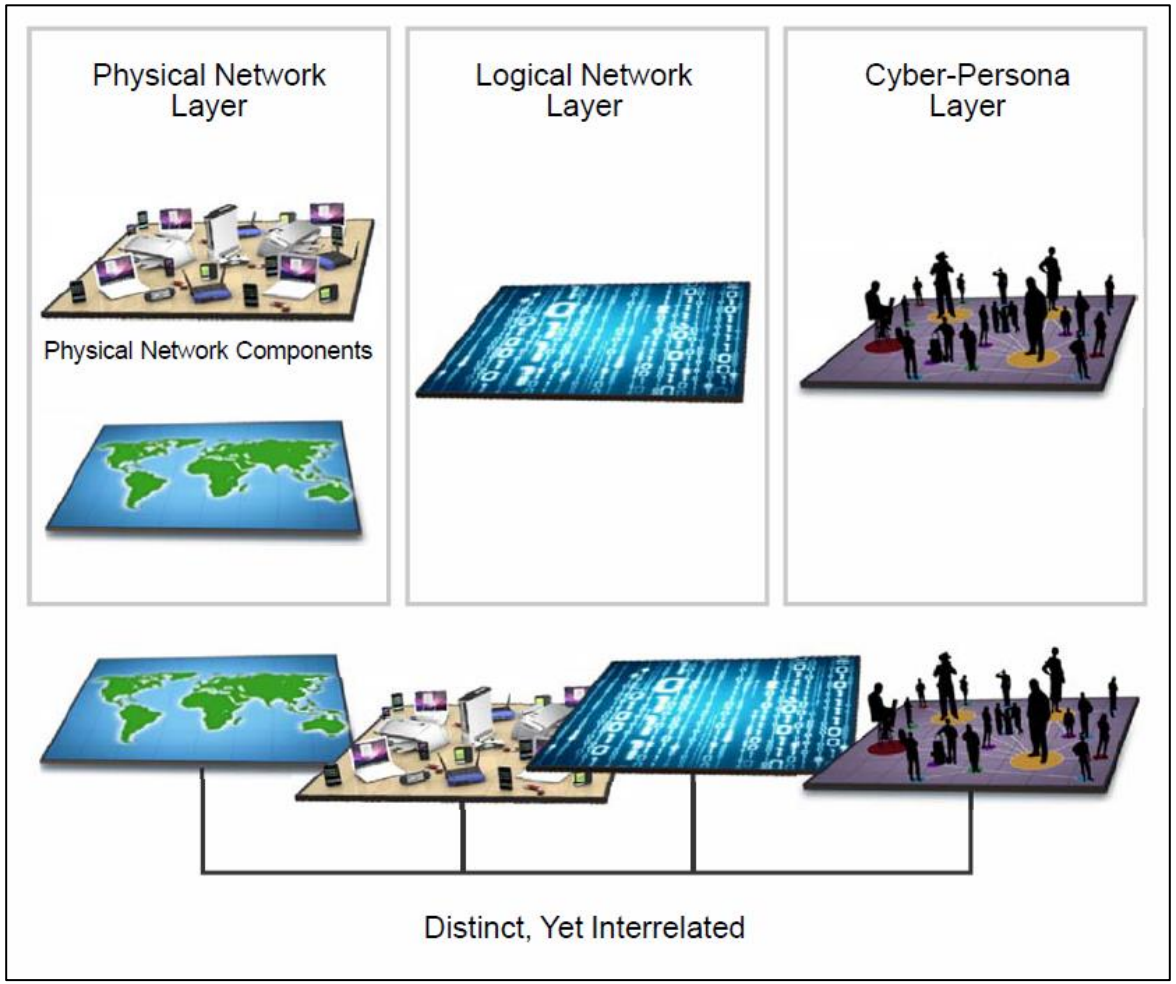


Image Source: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: Three Layers



Physical: Hardware providing storage, transport, and processing of information

Logical: Abstracted elements – data, code/applications, and network processes

Cyber-Persona: Digital representations of an actor or entity (e.g. human or automated machine accounts)

Image Source: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: 3 Missions

Joint and Air Force Doctrine divides actions into 3 cyberspace missions:

- **Offensive Cyber Operations (OCO):** Missions intended to project power in and through cyberspace.
- **Defensive Cyber Operations (DCO)**
  - Missions to preserve friendly cyberspace capabilities and protect data, networks, devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.
  - Seek to defeat threats that bypass or threaten to breach security measures
  - Protective, investigative, and response actions
- **DODIN Operations:** Operations to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense (DOD) Information Network (DODIN).

- AFRL also addresses **Cyber Assurance**: Integrated components and processes that provide measurable and provable guarantees for current and future system architectures.

Source of doctrine definitions: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: DODIN

"Set of information capabilities and associated processes for collecting, processing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel…"

- Gov owned and leased
- Networked and stand alone
- Hardware, software, and data
- Classified and unclassified networks (NIPRNET, SIPRNET, JWICS, others)
- Specialized systems
  - Industrial control systems
  - DoD-owned smart phones
  - Platform Information Technology (PIT): Includes weapons systems
  - These days discussion around using smart watches and other wearables

Image Source: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: The Blue, Red, and Gray

Blue Space: "Areas in cyberspace protected by the US, its mission partners, and other areas the DoD may be ordered to protect."

- DODIN
- Critical Infrastructure
- Key Resources

Red Space: "Portions of cyberspace owned or controlled by an adversary or enemy."

Gray Space: All other cyberspace that doesn't fit into Red or Blue (e.g. commercial cloud).

Source of doctrine definitions: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: Cyberspace

Contested Cyberspace

- Adversaries attempt to D4M (deny, degrade, disrupt, manipulate, or destroy) DoD capabilities in cyberspace
- Systems must be developed considering the contested space

Key Terrain in Cyberspace (KT-C)

- Analogous to a hill in conventional warfare
- Terrain changes far more rapidly than landforms, buildings, etc.
- Ex. Router, Intrusion Detection/Prevention System, Firewall, C2 System
- Sometimes key terrain not owned or controlled by the DoD (e.g. SCADA system controlling power/electricity)

Source of doctrine definitions: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

Cyber Doctrine: Cyber Operations Challenges

COTS

- Foreign ownership and control
- Supply chain

Attribution

- Who did it?
- Difficult – methods for anonymity
- One mechanism of deterrence

Network and Infrastructure Vulnerabilities

- Currently favored measures for networks – firewalls, IDS/IPS, training
- Infrastructure - operator errors, industrial accidents, natural disasters, purposeful attacks

Source: *Joint Publication 3-12 Cyberspace Operations and Air Force Doctrine Publication 3-12 Cyberspace Operations*

The Problem with Cyber

99 little bugs in the code…

99 little bugs in the code

Take one down, patch it around

127 little bugs in the code…

(Anonymous internet joke)

The Problem with Cyber

- Why don’t people just build, configure, and use systems correctly in the first place?
- Are developers, system admins, and users uneducated, incompetent, or lazy?
- Why not create secure cyber systems?
- What constitutes the root cause of vulnerabilities?

The Problem with Cyber

- Ill-trained users?
  - I changed all my passwords to “incorrect” so the system will tell me “my password is incorrect”
- Incompetent system administrators?
  - Message box told me to contact the system administrator….I AM the system administrator
- Ignorant system owners/customers?
  - If the customer is always right, what happens when two customers disagree?
- Uncaring system developers and testers?
  - Worked fine in dev…ops problem now

The Problem with Cyber

- Users that forget or ignore training
- Customers that change what they want, want way too much too fast, and/or refuse to pay security costs
- Architects that create vulnerable architectures and designs
- Developers that write millions of lines buggy code and testers that fail to correct the mistakes
- Operators and administrators that forget or ignore training and configure systems in insecure states

The Problem with Cyber

- High complexity – systems with hundreds or thousands of subcomponents and millions of lines of code are too complex for the smartest humans to secure…times more thousands
- *"Complexity is the worst enemy of security, and it always comes in the form of features or options."* N. Ferguson, B. Schneier
- The rise in system complexity tends to outpace advances in cyber security
- The problem has grown worse as systems get more complex over time

The Problem with Cyber

"*Because of cyberspace's complexity, global superiority is not achievable. In some cases, even localized superiority may be impractical. To ensure success in joint all-domain operations (JADO), commanders should expect contested cyberspace operations and account for anticipated capabilities degradation.*"

Source: Air Force Doctrine Publication 3-12 Cyberspace Operations – 1 Feb 2023

The Problem with Cyber

- Vulnerabilities may be introduced at all stages of the System Development Lifecycle (SDLC)
- **Requirements / User Stories** – Missing, ambiguous, non-atomic, untestable, etc. requirements (e.g. no requirement for encryption on a command and control (C2) link)
- **Architecture and Design** – Separation of logic and data (e.g. separate sensor data from C2 data on a uncrewed aerial system (UAS))
- **Implementation** – Code-level issues (e.g. lack of input verification)
- **Deployment/Operation** – Configuration issues (e.g. misconfigured to enable FTP and anonymous access)

The Problem with Cyber: Paradigms

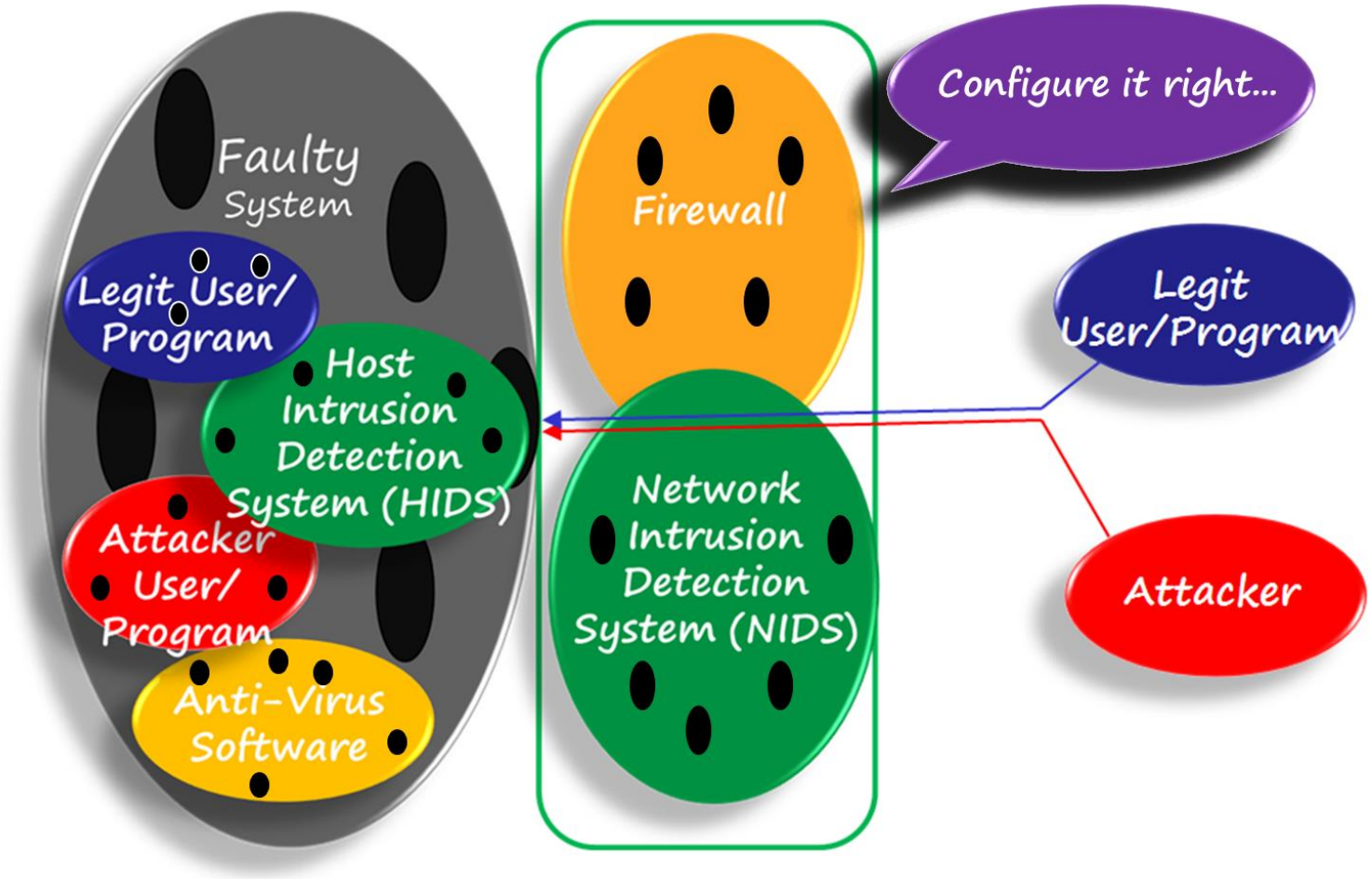
- Detect Paradigm: Use trusted security systems to monitor untrusted mission systems for malicious logic/behavior during operations
- Prevent Paradigm:
  - #1 Approach: Design and build trusted mission systems right so that malicious logic doesn't get on mission systems in the first place
  - #2 Approach: The overarching architecture and design enables leveraging untrusted components

The Problem with Cyber: Detect Paradigm

- Current approach: Secure highly complex and vulnerable systems by adding even more complexity and vulnerabilities to them (Firewall, IDS, AV)
- Security systems introduce additional vulnerabilities
- Security technologies are typically developed in the same manner as the technologies they attempt to protect
- Instances where the detection-based security systems introduce a single point of failure/juicy single target that threatens all systems
- Detect approach fails to detect novel threats
  - Paper estimated time from 0-day infect to detect is > 300 days

Adding complexity to solve a problem grounded in complexity?

The Problem with Cyber: Detect Paradigm



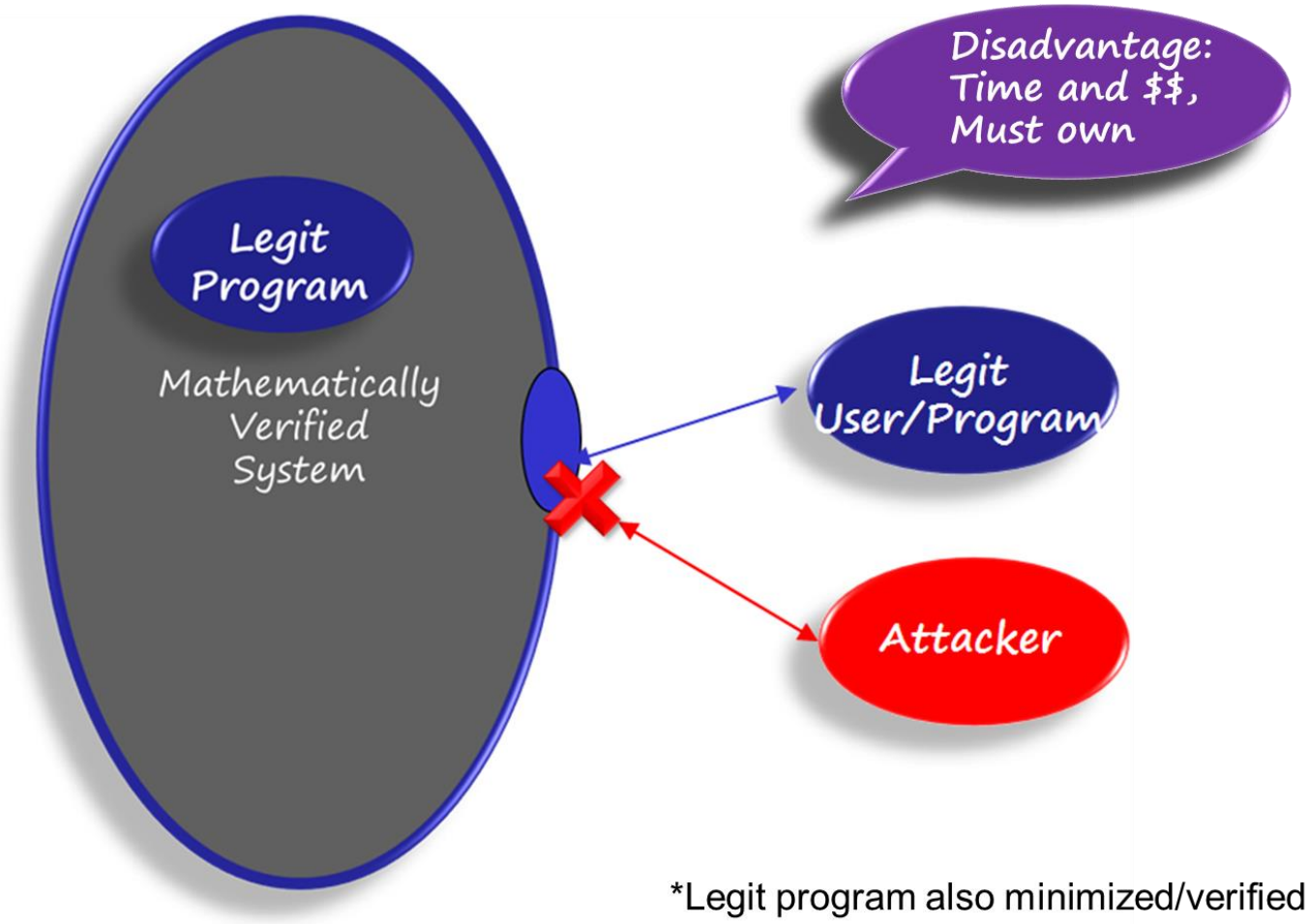
The Problem with Cyber: Detect Paradigm

- Detect-based solutions tend to friendly fire our systems
  - High CPU, memory, battery usage impacts functionality)
- Number of signatures continues to grow
- Adversaries test malware against all of these detect-based systems and modify to evade detection (this will include any AI-based detection systems)
- May lack signatures for highly specialized systems

The Problem with Cyber: Prevent Approach #1

- Simplify existing system, strip down to essentials (absolutely need vs nice to have, reduce complexity and connectivity, eliminate OS)
- Engineer in confidentiality, integrity, availability, authentication, authorization, attribution, etc.
- Red team the specification, architecture, and design (early-cycle CVA)
- Leverage formal methods: Specify system mathematically
  - Write proofs incorporating security properties and use an automated theorem prover
  - Define state machines and translate into the implementation
  - Verify implementation satisfies the specification

The Problem with Cyber: Prevent Approach #1



*Legit program also minimized/verified

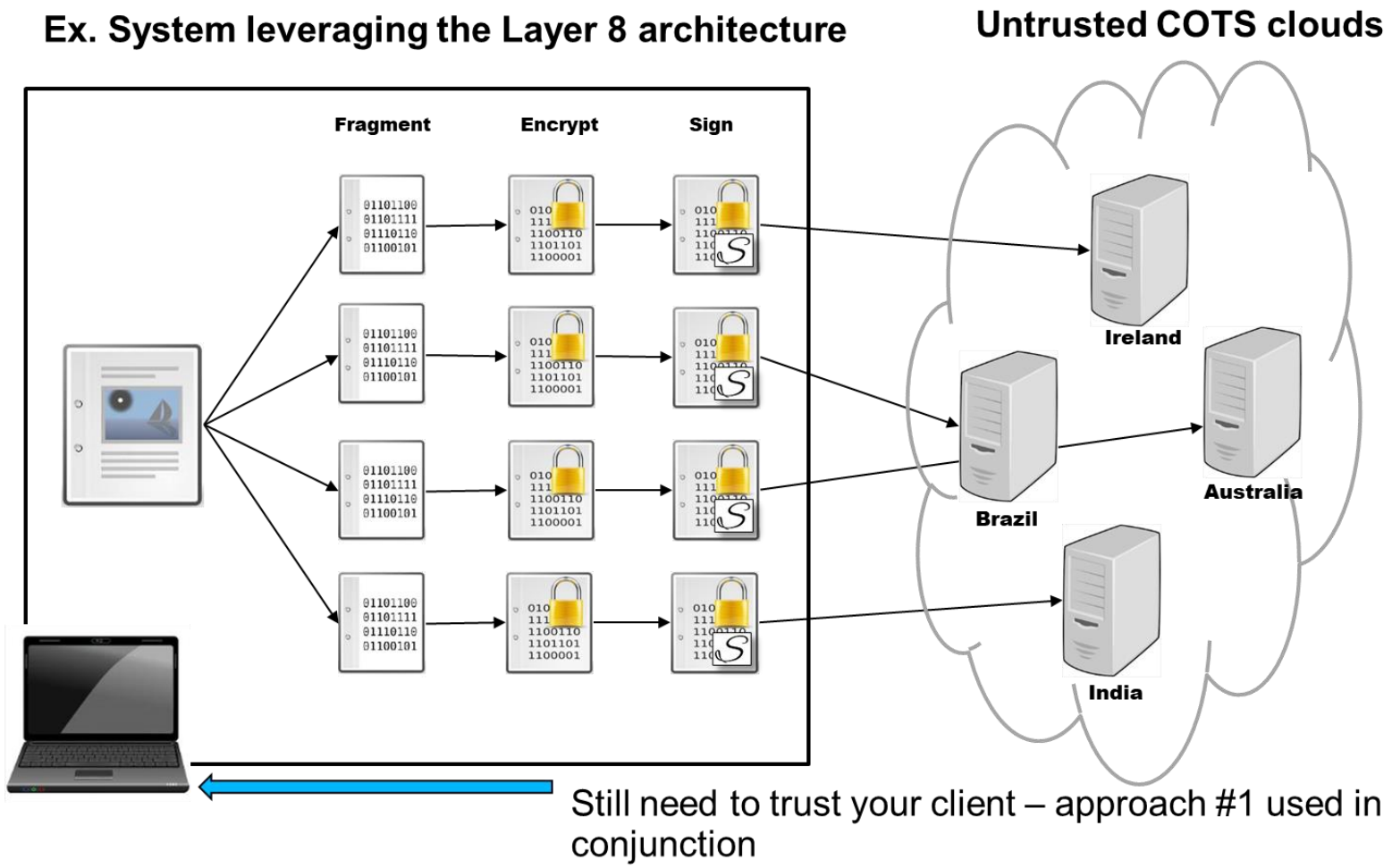
The Problem with Cyber: Prevent Approach #1

- Some systems are too complex to use this approach, but automated tools expanding capacity
- Ex. Windows 10 OS – ~50 mil lines of code, 100s of vulnerabilities
  - If estimate 1 vulnerability per 1000 LOC ~ 50,000 vulnerabilities
- Often, not much of an appetite for this approach – slow, $, reduces functionality
- Automated verification tools improve the speed and cost
- But technology adoption trends involves moving from GOTS to COTS

The Problem with Cyber: Prevent Approach #2

- Moving toward leveraging untrusted commercial assets like routers, communication links, and cloud servers
- If we do not specify, architect, design, or build our systems, we require another paradigm
- How can organizations safely leverage untrusted commercial assets for storing and sharing data?

The Problem with Cyber: Prevent Approach #2



RESCU Clouds – Effort that seeks to outsource storage and computation to assumed untrusted cloud notes

The Problem with Cyber: Final Thoughts

- Key points on complexity:
  - "Complexity is the worst enemy of security, and it always comes in the form of features or options." N. Ferguson, B. Schneier
  - The rise in system complexity outpaces advances in cyber security
- There are "solutions," but many are unpalatable or unworkable
- Classic argument: Formal modeling is too difficult to do on highly complex systems
- Counter-argument: If a system is too complex to formally model, perhaps we don't want to rely on it for the most critical operations
- Additional measures (e.g. disaggregation, redundancy, homomorphic encryption, etc.) to overcome lack of trust are currently being researched

2023 VICEROY MAVEN SUMMER INTERNSHIP

- 45 first-year interns, 5 graduate assistants
- 12 June - 4 August 2023 in Rome, NY
- Leadership, writing, public speaking, research, capstone, and graduation dinner components
- New for 2023
  - AF/SF mission and electromagnetic spectrum (EMS) emphasis
  - Cyber and EMS-focused lectures on UAS, Satellites, Cyber-Enabled Munitions, SCADA, and Military IoT
  - Blue Book® cyber vulnerability assessment of a mission system
  - IEEE conference-style paper on research projects
  - Hands-on cyber and EMS exercises

MAVEN MISSION, VISION, AND CORE VALUES

- **Vision**: Military, civilian, and industrial base sectors bolstered by a network of VICEROY Cyber Mavens
- **Mission**: Shepherding the next generation of cyber leaders into military, civilian, and industrial base sector careers
- **Core Values**
  - Diverse technical acumen
  - High-stakes problem solving
  - Effective leadership and followership
  - Respect for national imperatives and capabilities

2023 WEEKLY SCHEDULE RHYTHM

Time	M	T	W	H	F*
0800-1200	Lecture, IEEE and Blue Book® Drafts Due, Elevator Pitches, Lecture, Blue Book® Section Tasking B106 Aud	Research, Work on IEEE paper	Research, Work on IEEE paper	Research, Work on IEEE paper	Cyber Exercises Urtz
1300-1700					Lunch & Learns EMS Exercises Urtz

Questions

Thank you for your time!

Sonja Glumich
sonja.glumich@us.af.mil

Air Force Research Laboratory Information Directorate
VICEROY Air Force Program Manager