Cybersecurity
A Systems Perspective

DYNAMIC POSITIONING CONFERENCE
October 09 - 10, 2018

Paul Mario Koola Ph.D., MBA
Professor of Practice
Texas A&M University
Outline

• Introduction
• Cyberspace
• Complex Adaptive Systems (CAS)
• Subsystems & Trust
• Modeling Cybersecurity
• Future Possibilities
• Conclusions & Discussions
Cyberspace – 30,000 Feet View

• Reaches all corners of human access
• Combines interconnected devices into one **virtual entity**
• Cyber-Physical Systems (CPS)
  • Communication Networks, Power Grids, Transportation Networks, Ports and Shipping, **Dynamic Positioning Systems** ….
  • Internet – **Communication & Computation**
  • Industrial Internet of Things (IIoT) - SENSORS & ACTUATORS - + **CONTROL**
• Complex, Adaptive, Networked System
  • Information Exchange & Behavior Propagation → **Space & Time**
  • Similar to Human Body & Societies – Self Similarity
Cyberspace

1. Computation
2. Communication
3. Control
Complex Adaptive Systems (CAS)

• Systems Models
  • Heterogeneous Parts
  • Adaptive
  • Self Organization
  • Complexity – Local Rules produce Global Behavior
  • Emergence - Phase Transition

• Individual parts **DO NOT** add up to total system behavior

• Examples:
  • Social Networks; Power Grids; **Animal Swarms**; **Traffic Flows**; The Internet and Cyberspace
Bundles of birds in the sky figurine created a giant bird
https://daily.jstor.org/how-do-fish-schools-work/
The MarineTraffic terrestrial-based AIS network provides coverage of vessel positions in real-time at several thousands of ports and coastal shipping routes worldwide.

Autonomous Ships - Rolls-Royce

Forget Autonomous Cars—Autonomous Ships Are Almost Here

https://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous-ships-are-almost-here
DP → System of Systems

- Error Correction
- Reference Station
- GNSS Satellite
- Weather
- Inmarsat
- Transponder
- Cracker

Drilling Platform
- Azimuth Propulsion
- Mooring Tools
- Dynamic Positioning
- Science Capability
Cybersecurity

• Security is a System Property
  • DP Ship – System of Systems
  • DP Ship connected to other Systems
  • Links
    • Sensors (Weather) + Communication & Control
    • Physical [People & Goods (Viruses – Air/Water, Food & USB)] + Crackers

• Security is a Negative Goal
  • Is it possible to prove that no unauthorized person can take control of a DP Ship?
  • Burden of Proof – too HIGH
  • DP ships generally more robust
    • Sensor Fusion → GPS + Acoustic + Inertial + ..
    • Design Intent – Performance, Ease of Use OR Security?
  • Can we make it more secure – If so how?

• With a Lion and a Colleague – just need to outrun your colleague
  • Stronger DP means other Ships will be targeted
DP REFERENCE SYSTEMS – Current

• Critical to DP as vessel position used to control thrusters
• Hence multiple reference systems

• SENSOR FUSION
  • Commensurate - (GPS, Glonass, Beidou and Galileo)
  • Non-Commensurate (GNSS, Acoustic, Inertial)

• MODEL FUSION
  • Signal Processing Algorithms
  • Hierarchical Rules → @ Failure Weight Trustworthy Sensors

• Can we improve on this
  • US Joint Directors of Laboratories (JDL) Data Fusion – Military Applications
The Seven Pillars of DP Design & Security

- Autonomy
- Independence
- Segregation
- Differentiation
- Fault Tolerance
- Fault Resistance and
- Fault Ride Through

Focus on “Outcome”

1. Performance - Disturbances
2. Ease of Use
3. Security - Malicious

Integrity of a Fault Tolerant DP
PREDICT PROVE PROTECT

DISTRIBUTED rather than CENTRALIZED
Subsystems & Trust

Sensor:
  Faulty versus being Fooled
  Jamming versus Spoofing
Node - Abstraction

- Nodes
  - Computation & Control + Transducers (Sensors + Actuators)
  - Human: Brain + 5 Senses (Sight, Touch, Hearing, Taste, and Smell) + Limbs
  - Commensurate Vs Non-Commensurate Sensor Fusion

- Computation & Control
  - Hardware, Operating System (OS) and Application Software
  - Fast $\rightarrow$ Medium $\rightarrow$ Slow
  - Least Flexible $\rightarrow$ Most Flexible

- Transducers
  - Smart Transducer Standards - IEEE 1451.X

- Client or Server
  - GPS
Network Communications

• Drums used in Tribes and Horns on Ships
• Telegraph → Telephone → Radio
• Wired
  • Human Analogy: Nerves
  • Cable, Fiber
  • Electric, Electromagnetic (optical), Acoustic
• Wireless
  • Human Analogy: Sight, Hearing
  • Air, Water (liquid), Earth (seismic)?
  • Electromagnetic, Acoustic
• Intercepted, Jammed or Tampered
• CIA Triad
  • Confidentiality of information
  • Integrity of information, and
  • Availability of information
• Encryption
Trust in Network (not part of IP Protocol)

- Tribes
  - Eliminate untrustworthy tribesmen
- Society
  - Laws & Punishment
- Nations
  - Treaties & War
- Cyber
  - Spans across Groups & Nations – no single control authority
  - Virtual Assets
  - Technology growing faster than Laws & Policies
  - Ethics – Cyberweapon
- IP guaranteed to pass information if path available
IT versus OT - Security

• Computing Devices & Networks (IT)
  • Storing, Processing and Transmitting Information
  • Secure Information

• Cyber Physical Networked Systems (OT)
  • Temporal Behavior or Dynamics
  • Secure Dynamics
Model Fidelity – Trade Offs

<table>
<thead>
<tr>
<th>Attribute Details</th>
<th>Number of Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>Insufficient Details</td>
</tr>
<tr>
<td></td>
<td>Expensive to Compute</td>
</tr>
<tr>
<td>HIGH</td>
<td>Not Representative</td>
</tr>
</tbody>
</table>

- Insufficient Details
- Not Representative
- Expensive to Compute
1. High Level Model - Virus on a Network

- NetLogo: Multi-Agent Programmable Modeling Environment
- Network [Nodes & Links]
  - Biological
  - Cyber
- SIR
  - Susceptible
  - Infected
  - Resistant

(NetLogo: Stonedahl and Wilensky 2008)
2. SysML To Graph Based Model

2.... Graph to Vulnerability

• Databases that are hierarchical and interconnected
  • Common Attack Pattern Enumeration & Classification (CAPEC) – capec.mitre.org
  • Common Weakness Enumeration (CWE) - cwe.mitre.org
  • Common Vulnerabilities and Exposures (CVE) - cve.mitre.org
  • CVE-SEARCH PROJECT, cve-search.org

• System Model $\rightarrow$ Historic Attack Vector Databases
  • Assume System vulnerability
    • If attack vector from the databases maps to attribute of the system model

• Enables Security by Design

• Zero-day vulnerability not possible
3. Dynamic System Model

\[ \frac{dx}{dt} = Ax + Bu \]
\[ y = Cx + Du \]

Continuous-Time State-Space Model

Observability is a measure for how well internal states of a system can be inferred by knowledge of its external outputs.

• \( x \) is the state vector
• \( u \) is the input vector
• \( y \) is the output vector
• \( A \) is State Matrix, \( B \) is Input Matrix, \( C \) is Output Matrix, and \( D \) feedthrough Matrix

3. Dynamic Model - Security

- **Asymmetry** – Offense Vs Defense
- External Adversaries Perspective
  - Network Topology (Structure) and Dynamics are hidden
  - Can limited Observation from minimal nodes get above info
  - Without changing Structure & Dynamics in Complex Stochastic Systems
- Security Analysis
  - Metrics – Difficulty of Obtaining Structure & Dynamics Info
  - Models for Attack
  - Use in Model Fusion
Principles To Secure Cyber Systems

• **Proactive Security Measures**

• 1. Prevention
  • Complete Mediation, Separate Privilege, Principle of Least Privilege

• 2. Resilience Under Attack
  • Encryption
  • Redundancy in Subsystems (Fault Tolerance) – Marine Systems

• **Reactive Security Measure**

• 3. Recovery After Attack
  • 1) Detect 2) Isolate and 3) Recover
  • E.g. AntiVirus – Restoring - Safe Checkpoint State
Future Possibilities

• Quantum
  • Computation - superposition - parallel computations. D-Wave?
  • Communication – Entanglement Einstein’s “spooky action at a distance”
    • Chinese - information across 1200 kilometers - ultra-secure data transfer
  • Encryption

• Multiparty Computation
  • Fully homomorphic encryption

• Artificial Intelligence (AI) & Machine Learning (ML)
  • Anomaly detection, zero-day attacks, Behavioral analytics

• Blockchain

• Ethics – Cyberweapons, Laws & Policies
Conclusion

Higher Level Systems Model Fusion make the problem of attacking CPS Asymmetric.

This makes the adversaries job more difficult.
Q & A

Paul Mario Koola
paulmkoola@tamu.edu