GCOR XV, June 10, 2021

Complexity is the new Cyber Adversary

Robert K Gardner, Founder, New World Technology Partners; Max Planck, PhD. Technical Director Institute for Complex Additive Systems Analysis; Tom Walheim, Scientist/Staff Engineer - Cyber Systems L3 Harris Technologies; Greg Witte, Senior Security Engineer Huntington Ingalls Industries

The cascading risk that made Lehman Brothers infamous for accelerating the global financial crisis or the Northeast Power Outage that disabled parts of US and Canada in 2003 exemplify how counterparty risk turns a single breach into a disastrous systemic failure. Cyber risks face similar consequences. They are not enabled simply by individual cyber vulnerabilities, but by the Complex Systems-of-Systems they inhabit. Composed of legacy and new HW, SW and IoT elements connected by myriad channels, haphazardly integrated over many years, they lead to exploitable, accidental (even spontaneously combustible) systemic risks. This is not a computer science issue - it's a system engineering issue and there are solutions.

They begin with accurate models of system behavior and breach consequences. For the past 80 years, complex communications, weapons and industrial systems faced system reliability failures which were (and still are) addressed by legacy system engineering protocols such as Failure Modes Effects and Criticality Analysis (FMECA). Similar approaches may enable the design (and evolution) of cyber architectures which can absorb and operate through attacks as they occur, preventing impact propagation (and exhausting adversaries' resources). CISOs can and must expand their talent pool and their risk management perspective accordingly.

Learning Objectives:

- Understand how enterprise vulnerability increases due to system & application complexity
- Understand how usage load and tolerance issues exacerbate vulnerability
- Learn how you can integrate resilience to reduce potential systemic risk in complex systems

Content questions:

1. Beside adversaries and operator errors, how do new and emerging technologies threaten cyber system efficacy?
   a) IoT (Internet of Things) presents real-time actions that may not be prevented or caught before irrecoverable damage is done.
   b) Wireless communication hides attackers
   c) Artificial Intelligence (AI) uses 3rd party algorithms that often contain malware
   d) Totality of new and varied technologies and interconnections expands "threat space" beyond the ability to defend systems

2. How can complex systems achieve resilience?
   a) Provide a rapid incident response capability
   b) Make all critical systems redundant
   c) Evolve system architectures into isolatable islands
   d) Employ anomaly detection software tools

3. In systems with expanding complexity and real-time activity, traditional redundancy presents more perils than remedies, because (select all that apply):
   a) Redundant systems increase threat space and concomitant vulnerability
   b) Redundant hardware and software decreases reliability
   c) Backup systems reduce system performance
   d) Single points of failure are introduced

4. How does supply chain risk exacerbate complex cyber systems?
   a) Suppliers and their suppliers troll your other suppliers to identify unprotected access points
   b) Cyber intrusions to counterparties may trigger counterparty risk events that propagate into your systems and assets
   c) Clients who for which YOU are in their supply chain can reach back into your enterprise