Measuring Cyber-Physical Resilience: Modeling, Formulation and Analysis

Venkatesh Venkataramanan

ESIC Seminar
09/29/2020
Motivation
Problem Description and background
Cyber-Physical System modeling – why is it hard?
A story about choice
A closer look at threats
Summary
DOE/NERC High-Impact Low Frequency Events
More catchy news – Triton, Industroyer, Ransomware

Reports of ICS Malware

STUXNET 2010
HAVEX 2013
BLACKENERGY 2015
IRONGATE 2015
INDUSTROYER 2016
TRITON 2017
Problem description and background
Why do we need resilience?

“Security of any system can never be perfect. So it always must be weighed against other priorities -- such as *speed, flexibility and ease of use* -- in a series of inherently nuanced trade-offs” – *Linus Torvalds* [Emphasis added]

*Quis custodiet ipsos custodes?*
What is cyber-physical resiliency?

Nobody knows yet for sure
Definitions of cyber-resilience

1. the ability to recover and resume operations within acceptable levels of service.
2. a cyber system’s ability to function properly and securely despite disruptions to that system.
3. a holistic view of cyber risk, which looks at culture, people and processes, as well as technology.
4. A system’s ability to withstand cyber attacks or failures and then quickly reestablish itself.
5. ability of systems and organizations to withstand cyber events.
6. ability to withstand and recover quickly from unknown and known threats.
7. an organization’s ability to recover and return to normal operations after a cyber attack.
8. an organization’s ability to respond to and recover from a cybersecurity incident.
9. the ability to provide and maintain an acceptable level of service when facing attacks and challenges to normal operation.
11. the ability of systems and organizations to withstand cyber events.
12. the ability to withstand attacks and failures, as well as to mitigate harm more than in other domain.
13. the capability of a supply chain to maintain its operational performance when faced with cyber-risk.
14. the capacity to recover quickly from difficulties; toughness.
15. the continuation of operations even when society faces a severe disturbance in its security environment, the capability to recover quickly from the shock, and the ability to either remount the temporarily halted functions or re-engineer them.
16. the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.
17. the ability to adapt and respond rapidly to disruptions and maintain continuity of operations.
18. the ability to continuously deliver the intended outcome despite adverse cyber events.
19. the ability to operate in the face of persistent attacks.
20. the ability to prepare for and adapt to changing threat conditions while withstand and rapidly recovering from attacks to infrastructure availability.
21. the ability to prepare for and recover quickly from both known and unknown threats.
22. the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
23. the ability to recover from or easily adjust to misfortune or change.
24. the ability to recover, returning to an original state, after some event that disrupts this state.
25. the ability to withstand attacks and failures, as well as to mitigate harm more than in other domain.
26. the capability of a supply chain to maintain its operational performance when faced with cyber-risk.
27. the capacity to recover quickly from difficulties; toughness.
28. the ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities conditions, stresses, or attacks on the supporting cyber resources it needs to function.
29. the ability of a substance or object to spring back into shape.
30. the ability of a system that is dependent on cyberspace in some manner to return to its original or desired state after being disturbed.
31. the ability of an organization to understand the cyber threats it’s facing, to inform the known risks, to put in place proportionate protection, and to recover quickly from attack.
32. the ability of an organization to continue to function, even though it is in a degraded manner, in the face of impediments that affect the proper operation of some of its components.
33. the ability of cyber systems and cyberdependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats.
34. the ability of systems and organizations to develop and execute long-term strategy to withstand cyber events.
35. the ability of systems and organizations to withstand cyber events.
36. the ability of systems and organizations to cope with cyber attacks.
37. ‘robustness’ and ‘survivability’ measured in terms of performance and sustained availability. It also implies elements of both confidentiality and integrity.
38. maintaining the system’s critical functionality by preparing for adverse events, absorbing stress, recovering the critical functionality, and adapting to future threats.
39. the ability to anticipate, withstand, recover from, and evolve to better adapt to advanced cyber threats.
40. the ability of systems and organizations to develop and execute long-term strategy to withstand cyber events.
41. the ability to prepare for and adjust to changing conditions and withstand and recover rapidly from disruptions.
42. the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
43. the ability to continue to operate in the face of persistent attacks.
44. the ability to continuously deliver the intended outcome despite adverse cyber events.
45. the ability to operate in the face of persistent attacks.
46. the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
47. the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.
48. the ability to provide and maintain an acceptable level of service when facing attacks and challenges to normal operation.
49. the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.
50. the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
51. the ability to recover from or easily adjust to misfortune or change.
52. the alignment of prevention, detection, and response capabilities to manage, mitigate, and move on from cyberattacks. It is the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks.

Courtesy - Aaron Clark-Ginsberg (Stanford, DHS) “What is cyber-resilience?”
**Resilience – current work**

Physics based resilience – usually calculated in terms of time

An intrusion tolerance architecture that uses control-theoretic decision making to select optimal response strategies

**Cyber-Physical Resilience: Definition and Assessment Metric**

Andrew Clark, Member, IEEE, and Saman Zonouz, Member, IEEE

**Resilient Control Systems**

Practical Metrics Basis for Defining Mission Impact

Craig G. Rieger
Senior Member, IEEE
Idaho National Laboratory
Idaho Falls, Idaho, USA

Towards Cyber-Physical Intrusion Tolerance

Shamina Hossain, Srijanha Etigomi, Kate Davis, Saman Zonouz
Electrical and Computer Engineering Department
University of Illinois, *Rutgers University*
{shossai2, krogers6}@illinois.edu, {se260, saman.zonouz}@rutgers.edu
Cyber-physical models
How are they different?

<table>
<thead>
<tr>
<th>S. No</th>
<th>Characteristics</th>
<th>Physical System</th>
<th>Cyber System</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Components</td>
<td>Generator, Transformer, Transmission Line, Circuit Breaker, Protective Relay, Load, etc.</td>
<td>Control Systems, Computing Devices, Communication Networks</td>
</tr>
<tr>
<td>2.</td>
<td>Nature of System</td>
<td>Continuous, Dynamic behaviour</td>
<td>Discrete, Static behaviour</td>
</tr>
<tr>
<td>4.</td>
<td>System State</td>
<td>Energy Flow</td>
<td>Information Flow</td>
</tr>
<tr>
<td>7.</td>
<td>Contingency</td>
<td>Physical Contingency</td>
<td>Cyber Contingency</td>
</tr>
<tr>
<td>8.</td>
<td>Types of Contingency</td>
<td>Line Fault, Generator Outage, Load Outage, Environmental effects, etc.</td>
<td>Cyber Attacks, Communication Latency, Malicious Control effects, etc.</td>
</tr>
<tr>
<td>10.</td>
<td>Event Synchronization</td>
<td>Asynchronous</td>
<td>Synchronous</td>
</tr>
</tbody>
</table>
**Mathematical modeling**

\[
\begin{align*}
\min_{y \in \mathbb{R}^N} & \{ f(y) \} \\
\text{s.t.:} & \\
& h_j(y) \leq 0, \quad 1 \leq j \leq M_h \\
& g_k(y) = 0, \quad 1 \leq k \leq M_g
\end{align*}
\]

A standard OPF formulation

\[
q^+ = \delta(q, v) \quad \zeta = K(q)(q, v) \in Q \times \Sigma
\]

A standard FSM formulation

- \(q\) – State
- \(\delta\) – State transition function
- \(K\) – Output function
- \(v\) – Input
- \(\Sigma\) – Set of all valid states
Captain America

- Solid and reliable
- Provides an excellent platform to build on
- How to deal with additional systems?
- How to deal with interactions?
- How to deal with increased scale, and explosive amounts of data?
- Needs an update for the digital era
Compromise – topology mapping
The cyber model needs to incorporate two key properties — a) inter-depending between systems b) range of impact from attack

Power system graph is a *graph minor* of the communication graph

The graphs are also assumed to *isomorphic*, and a bijective mapping is assumed between the two graphs

\[ f : G_p \rightarrow G_c, \mid (x,y) \in G_p \Rightarrow (f(x), f(y)) \in G_c \]
Reachable machines

- The reachable machines in a domain are the machines that can be accessed without additional security privileges.

\[ RD = G_s \subset G_c \ni S \rightarrow 1 \]

- It can model regular operation and malicious activity.

- The mapping is a combination of the cyber and communication models.

- In addition to the processes/devices in a physical node, there are also communication links between the nodes.

- Graph \( G_s \) expands with accumulated attacker privileges.

- The concept of reachable machines is used to determine the impact of a successful exploit.
Cyber-physical dependence

Network Diagram:
- **CONTROL CENTER (CC)**
  - **SUBSTATIONS** (SS1, SS2, SS3, SS4, SS5, SS6, SS7)
    - **SWITCHES** (SW1, SW2, SW3, SW4, SW5, SW6)
      - **NODES** (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21)
End model - Glacier

System state needs to be updated regularly!
Need to also incorporate other elements – testbed plug

- Monitoring tools, and IDS to be deployed
- Distributed optimization based reconfiguration, avoiding single point of failure
- Simulation Tool
- Data Flow
- Attack Packets
- Attack Agent(s)
- Monitoring tools, and IDS to be deployed
- Monitor Power System Impact

- OPC Interface And other Protocols, such as IEC 61850
- CORE Emulation
- Or Mininet

- ListenOnPort Interface
- And other interfaces, including NIC and CHIL

- Application Layer
- Communication Layer
- Power System and Sensor Layer

- Resiliency based Reconfiguration
- New Switch Status
- Control Algorithm in Python

- RTDS
- Opal-RT
Problem – how to combine?
Cyber-Physical Security Assessment Metric (CP-SAM)

- Integrate measurements, computed parameters, and weights with Fuzzy Choquet Integral
- Scale resiliency value between (0-100)
What, Why, and How - Choquet Integral?

What?
• An integral that is used to as a way of measuring the expected utility of an uncertain event

\[ C_\mu(f) = \int f \, d\mu = \sum_{i=1}^{n} (f(x_i) - f(x_{i-1})) \mu(A_i) \]

Why?
• Resiliency is a qualitative measure – there is no direct quantification
• Resiliency is subjective – preferences and definitions vary

How?
• How do we understand which factors contribute to resiliency in a particular scenario?
• We define an interaction index – positive, negative, or zero interactions are defined between factors
Simple formalization of the problem

- maximize (minimize) \[ \sum_{i=1}^{m} w_i x_i \] subject to

\[ w_i \geq 0 \]
\[ \sum_{i=1}^{m} w_i = 1 \]
\[ \sum_{i=1}^{m} w_i r_i \leq \text{risk} \]
\[ \sum_{i=1}^{m} w_i R_i \geq \text{return} \]

- Goal: find the vector \[ w = (w_1, \ldots, w_m) \]
Existing techniques

- Payoff-based strategies

- Methods involving stochastic processes

- Intelligent systems techniques
  - Genetic algorithms
  - Rule-based expert systems
  - Neural networks
  - Support vector machines
Drawbacks of the existing techniques

- Learn from examples:
  - Overfitting data

- Ignore relationships among characteristics of an asset:
  - Higher risk usually implies higher return
  - Longer time to maturity usually leads to higher risk

- Assume precise data:
  - Return expected by an investor
  - Return and risk associated with an asset
Tools for a novel approach

- Multi-criteria decision making
- Fuzzy measure and fuzzy integration:
  - Take care of dependence among characteristics
- Intervals:
  - Take care of imprecise data
Multi-criteria decision making

- Comparison of multidimensional alternatives to select the optimal one
  - Pick the best control action possible

- Elements of a MCDM setting:
  - a set of alternatives
    - Various control actions (finitely many)
  - a set of criteria
    - Cost, stability constraints, operation constraints, contracts, and so on
  - a set of values of the criterion
    - payoff=[0,50], time={1,2,3}, reputation={bad, average, good}
  - a preference relation for each criterion

- Challenge: Combine partial preferences into a global preference
Utility function

- Utility function is a transformation from an ordered set to a set of real numbers.

- Construct a utility function for each criterion that maps values of all criteria to a common scale.

- Combine monodimensional utilities into a global utility function using an aggregation operator. How?
Combining monodimensional utilities

- Maximax approach
  - Optimistic situation

- Maximin approach
  - Pessimistic situation

- Weighted sum approach
  - Advantage: simple to calculate, $O(n)$
  - Disadvantage: ignores the dependence among criteria
    - Longer time to maturity $\rightarrow$ higher return
Fuzzy integration: the Choquet integral

- Decision maker inputs value of importance of each subset of the set of criteria

- The Choquet integral is an aggregation operator evaluated w.r.t. a non-additive measure, which is defined by the values of importance of (subsets of) criteria

- Drawback: exponential complexity
2-additive measure

A non-additive measure where all interaction indices of order 3 and higher are null, and at least one interaction index of order 2 is not null.

Advantages of using 2-additive measure:
- Lower complexity than non-additive measure
- Takes into consideration dependence among criteria

The Choquet integral w.r.t. a 2-additive measure:

\[
(C) \int f \, d\mu = \sum_{I_{ij}>0} (f(i) \land f(j))I_{ij} + \sum_{I_{ij}<0} (f(i) \lor f(j))|I_{ij}| + \sum_{i=1}^{n} f(i) \left( I_i - \frac{1}{2} \sum_{i \neq j} |I_{ij}| \right)
\]

Decision-maker inputs the importance of each attribute and the importance of each pair of attributes
Intervals

- A real interval $[x, x]$ is a closed and connected set of real numbers.
- Calculate the Choquet integral w.r.t. a 2-additive measure over intervals.

Advantages:
- Considers the interactions among attributes
- Quadratic complexity

Drawback:
- Imprecise values of importance and interaction indices
Cyber-Physical Resiliency

- Edge Count
- Overlapping Edges
- Switching Operations
- Repetition of Sources
- Centrality
- Probability of Availability
- Penalty Factor

Weights assigned to factors using pairwise comparison, or can be used defined according to requirement

Interaction Index $\lambda$ is determined – models interdependency between factors considered

$$C_{\mu}(f) = \int f d\mu = \sum_{i=1}^{n} (f(x_i) - f(x_{i-1})) \mu(A_{(i)})$$

Choquet Integral to combine the factors into single resiliency value

Courtesy – Sayonsom Chanda, WSU
What about cyber-attacks?
“I sent my bank details and Social Security number in an e-mail, but I put ‘PRIVATE FINANCIAL INFO’ in the subject line so it should be safe.”
Growth of Cyber Threats

Advanced Persistent Threat (APT)

**Advanced**
- Well funded, professionals
- Uses zero-day vulnerabilities
  - Vulnerabilities discovered by an attack, but unknown to defender
- Will have sophisticated rootkits to hide attacks
- Will utilize covert methods to attack and exfiltrate data
- Will perform heavy reconnaissance of organization (both technical and personal)

**Persistent**
- Will continually attack until successful
- Understand “Law of large numbers”

https://www.slideshare.net/GTSCoalition/robert-carey-principal-cio
Cyber Security Properties

Confidentiality
“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”

Integrity
“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity”

Availability
“Ensuring timely and reliable access to and use of information.”

CIA Triad
NIST FIPS-199

Example #1: SC SCADA System = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}

Attack?

1) Denial of Service
Prevent/delay authorized communication

2) Eavesdropping
Unauthorized observation of information sent over the network

3) Spoofing
Message sent with false source

4) Man-in-the-Middle
Attacker can receive, alter, and resend data

Source → X

Destination
Attackability

System’s Surface (e.g., API)

Attacks

Intuition

Reduce the ways attackers can penetrate surface

→ Increase system’s security
Framing the problem

What keeps you awake at night?

- How effective are my defenses?
- Can I detect WireBitingSquirrel, RampaginHippo, or whatever the latest APT of the hour is?
- Is the data I’m collecting actually useful?
- Do I have obvious gaps? Do I have overlapping tool coverage? If so, how much?
- Will this *shiny new* product from a vendor in the lobby really help power grids’ defenses?
WHAT is ATT&CK?

- **ATT&CK IS NOT** – An open-source (or any other kind of) threat intelligence feed full of IOCs to look for

- **ATT&CK IS NOT** - Yet another kill-chain system that describes an event lifecycle

- **ATT&CK stands for** “Adversarial Tactics, Techniques, and Common Knowledge”

- **ATT&CK IS** - A globally-accessible knowledge base of adversary tactics and techniques, categorized into an easily-consumable model

- **ATT&CK IS** - Based on real-world in-the-wild observations of actual adversary behavior

- **ATT&CK IS** – Purposefully focused on the adversary and the behaviors they exhibit, tools they use, and actions they perform.

- **ATT&CK IS** – Community driven, and updated by MITRE quarterly based on new things being seen and reported in the wild.
How ATT&CK Is Laid Out

- ATT&CK is laid out as a series of adversary tactics, each of which are comprised of many techniques.
- Techniques are what one wants to detect/mitigate, and emulate when red teaming.
- This is often laid out in a tabular matrix form for ease of consumption.
- As part of ATT&CK, MITRE also describes the adversaries (80) and malware/tools (280) who use these various techniques.
ATT&CK and the Cyber Kill-Chain

- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities

- Stage Capabilities
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
What is a TECHNIQUE in ATT&CK?

<table>
<thead>
<tr>
<th>Technique</th>
<th>New Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>When operating systems boot up, they can start programs or applications called services that perform background system functions. […] Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools.</td>
</tr>
<tr>
<td>Platform</td>
<td>Windows</td>
</tr>
<tr>
<td>Permissions Required</td>
<td>Administrator, SYSTEM</td>
</tr>
<tr>
<td>Effective Permissions</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>Detection</td>
<td>Monitor service creation through changes in the Registry and common utilities using command-line invocation …</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Limit privileges of user accounts and remediate Privilege Escalation vectors…</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Windows registry, process monitoring, command-line parameters</td>
</tr>
<tr>
<td>Examples</td>
<td>Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, …</td>
</tr>
</tbody>
</table>
What is a GROUP in ATT&CK?

<table>
<thead>
<tr>
<th>Group</th>
<th>APT 28</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>APT28 is a threat group that has been attributed to the Russian government. This group reportedly compromised the Democratic National Committee in April 2016.</td>
</tr>
<tr>
<td><strong>Aliases</strong></td>
<td>Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group4127, TG-4127</td>
</tr>
<tr>
<td><strong>Techniques</strong></td>
<td>Input Capture - CHOPSTICK is capable of performing keylogging. Command-Line Interface - CHOPSTICK is capable of performing remote command execution. Fallback Channels - CHOPSTICK can switch to a new C2 channel if the current one is broken. Connection Proxy - CHOPSTICK used a proxy server between victims and the C2 server.</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>CHOPSTICK, JHUHUGIT, ADVSTORESHELL, XTunnel, Mimikatz, HIDEDRV, USBStealer, CORESHELL, OLDBAIT, XAgentOSX, Komplex, Responder, Forfiles, Winexe, certutil</td>
</tr>
</tbody>
</table>
What is SOFTWARE in ATT&CK?

<table>
<thead>
<tr>
<th>Software</th>
<th>CHOPSTICK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>CHOPSTICK is malware family of modular backdoors used by APT28. It has been used from at least November 2012 to August 2016 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases.</td>
</tr>
<tr>
<td>Aliases</td>
<td>CHOPSTICK, SPLM, Xagent, X-Agent, webhp</td>
</tr>
<tr>
<td>Techniques</td>
<td>• Data Obfuscation • Connection Proxy • Standard Application Layer Protocol • Remote File Copy • Rundll32 • Indicator Removal on Host • Timestomp • Credential Dumping • Screen Capture • Bootkit…</td>
</tr>
<tr>
<td>Groups</td>
<td>APT28</td>
</tr>
</tbody>
</table>
WHEN and WHERE would I use MITRE ATT&CK?

MITRE ATT&CK

- Detection & Analytics
- Evaluating Tools
- Measuring Defense
Our use-case: Measuring and Enabling Resilience

- Analytics **look for** observable events and artifacts that indicate adversary behavior.
- E.g., if an adversary uses RDP, Windows Event Logs will show a Login **with type=RemoteInteractive**
- Most analytics described in ATT&CK are **general purpose** and will result in **false-positives** if deployed in isolation.
- **Environmental context** is required to fill in the gaps.
- **#PROTIP** – Only **Groups** or **Chains** of successful analytics should lead you to increased confidence.
Summary

- Power grid models need to evolve to support modeling of complex, dynamical, interacting behavior.

- Analysis of inter-dependent behavior is a complex phenomenon – we need similar complex tools to draw insights.

- Cyber-attacks are coming – but don’t reinvent the wheel, call your IT help!
thank you.
vvenkata@mit.edu