SANDIA REPORT

SAND2018-3488
Unlimited Release
August 2017

Literature Review on Modeling Cyber Networks and Evaluating Cyber Risks

Andjelka Kelic, Philip L. Campbell
Contributors: Robert A. Taylor, Anita Bhat, Kevin L. Stamber

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy

Office of Scientific and Technical Information

P.O. Box 62

Oak Ridge, TN 37831

Telephone: (865) 576-8401

Facsimile: (865) 576-5728

E-Mail: reports@osti.gov

Online ordering: http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce

National Technical Information Service

5301 Shawnee Rd

Alexandria, VA 22312

Telephone: (800) 553-6847

Facsimile: (703) 605-6900

E-Mail: orders@ntis.gov

Online order: http://www.ntis.gov/search

SAND2018-3488
August 2017
Unlimited Release

Literature Review on Modeling Cyber Networks and Evaluating Cyber Risks

Andjelka Kelic, Philip L. Campbell
Contributors: Robert A. Taylor, Anita Bhat, Kevin L. Stamber
Resilience and Regulatory Effects, Networked System Survivability and Assurance
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS1137

Abstract

The National Infrastructure Simulations and Analysis Center (NISAC) conducted a literature review on modeling cyber networks and evaluating cyber risks. The literature review explores where modeling is used in the cyber regime and ways that consequence and risk are evaluated. The relevant literature clusters in three different spaces: network security, cyber-physical, and mission assurance. In all approaches, some form of modeling is utilized at varying levels of detail, while the ability to understand consequence varies, as do interpretations of risk. This document summarizes the different literature viewpoints and explores their applicability to securing enterprise networks.

ACKNOWLEDGMENTS

Funding for this work was provided by the Department of Homeland Security (DHS) Office of Cyber and Infrastructure Analysis (OCIA). OCIA provides innovative analysis to support public and private-sector stakeholders' operational activities and effectiveness and to inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis. The authors also wish to thank Louise Maffitt for her editing efforts on the document.

TABLE OF CONTENTS

FIGURES

This page intentionally left blank.

EXECUTIVE SUMMARY

NISAC was tasked with conducting a literature review on modeling cyber networks and evaluating cyber risks. The literature review to examined where modeling was used in the cyber regime and the methods used to examine consequence and risk. The relevant literature appears to cluster in three distinct areas: network security, cyber-physical, and mission assurance. Approaches in each of these spaces utilize some form of modeling at varying levels of detail, whether and how they determine consequence varies, as does the interpretation of risk. Each area is summarized briefly below. Network security literature primarily focuses on vulnerability and defense. Consequence is assumed. Cyber-physical literature touches on defense and vulnerability but is focused on understanding consequence. Mission assurance literature consider cyber as a supportive infrastructure; its focus is mitigating consequence.

Network Security

In the network security space, the research typically begins with the assumption that a network map is known and someone has decided in advance what is important to protect. Alternatively, in the space of network assessments and red teaming, the red team develops network maps as it acts as an adversary: the focus is managing risk by controlling the vulnerabilities and building better defenses.

Modeling is either (a) highly detailed and typically at the network traffic level (protocol and packets); or (b) involves the use of network diagrams or network graphs. Traffic-level models are used to develop better rules for tools such as intrusion detection systems or firewalls, or to increase situational awareness or the effectiveness of threat assessment tools. Network graphs look at the connectivity between nodes on the network. An important subtype is the “attack graph.” Red teams often construct attack graphs to guide their attack steps. Attack graphs can be used to assess areas where defenses could be most beneficial.

Cyber-Physical

Unlike modeling in network security, modeling in this space focuses on understanding attack impacts to the physical side of the cyber-physical system. The electric grid is the primary system of study, including both distribution and transmission grid models. Some modeling is highly detailed, similar to the network security space, and is used to investigate defense and vulnerability issues. These approaches model the control system, usually as coupled with business networks. However, more of the work in this space focuses on understanding a combination of the topology of the network and that of the grid itself, so the models are large scale with minimal physical detail. The goal is to gain a better understanding of the interconnectedness, potential attack impacts on reliability, and the consequences of a cyber event.

Mission Assurance

Literature in the mission assurance space considers cyber and cyber systems as supportive to a mission. Similar to the cyber-physical space, the focus is on consequence. Models in the mission assurance space tend to be process models or process diagrams. The focus on process allows risk to also be managed from the perspective of mitigating attacks or constructing the system or process such that the mission can still be achieved despite a successful attack.

This page intentionally left blank.

NOMENCLATURE

Abbreviation	Definition
DHS	Department of Homeland Security
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
NISAC	National Infrastructure Simulation and Analysis Center
NVD	National Vulnerability Database
OCIA	Office of Cyber and Infrastructure Analysis
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block

This page intentionally left blank.

1. INTRODUCTION

NISAC conducted a literature review on modeling cyber networks and evaluating cyber risk with an eye towards exploring the applicability of the approaches for use in evaluating cyber risk in enterprise networks. This document provides a summary of that review, categorizes the articles by areas of focus, and explores the type(s) of modeling used and how it is applied.

The project team began the search, as broadly as possible, in academic databases such as Compendex/Engineering Village and Web of Science. The searches were conducted using combinations of search terms such as: *cyber*, *network*, *security*, *simulation*, *model*, *enterprise*, and *risk* in various combinations to identify combinations yielding the most relevant results. For example, the Compendex/Engineering Village database lists 267 articles published in the last few years (2015-2017) that match the following search criteria:

model* AND simul* AND cyber AND network AND security

Many of the relevant articles had been published by the Institute of Electrical and Electronic Engineers (IEEE). By narrowing the search database to IEEE Xplore, the team was able to broaden the years of publication examined and use less restrictive searches. For example the use of OR as an operator with *model** and *simul** as search terms rather than AND still yields a tractable set of results.

The relevant literature seems to cluster in three different spaces: network security, cyber security as related to cyber-physical systems, and mission assurance. Approaches in each of these spaces utilize some form of modeling at varying levels of detail, whether and how they determine consequence varies, as does the interpretation of risk. Network security primarily focuses on vulnerability and defense. Consequence is assumed. Cyber-physical touches on defense and vulnerability but is focused on understanding consequence. Mission assurance considers cyber as a supportive infrastructure. Focus in this space is the mitigation of consequence. Some research articles overlap these focus areas and others address risk directly.

1.1. Risk

Risk is a function of threat, vulnerability, and consequence. All of the approaches discussed in the articles are fundamentally trying to manage risk. The approaches vary in the portion of the risk equation they address, but are consistent across the three categories. While threat is discussed, none address threat directly. There is an implicit assumption that threat is out of the control of risk managers who, at best, can obstruct attacks well enough to limit them to highly sophisticated and well-resourced adversaries.

Several authors attempt to explore threat by looking at the capabilities of adversaries. As part of characterizing threat, Duggan (2006) discusses the creation of generic threat profiles that incorporate the capabilities and resources available to different types of adversaries. Llansó (2015) considers attack-level-of-effort to be a component of likelihood and looks at tiers of attackers, their capabilities, and defense requirements to resist the capabilities.

In the network security realm, consequence is assumed. Some entity has already identified the system or component needing protection, the level of consequence, and likelihood of compromise. Thus the focus in this space concentrates on the vulnerability portion of risk and the attempt to harden systems as much as possible. Although some of the reviewed publications refer to this process as addressing threat, they then proceed to discuss threat as the level of effort

required for an adversary to achieve a goal. The focus is then on making that level of effort as high as possible by hardening the systems. Several authors also discuss the likelihood of attack (for example, Maggi 2008), but link attack likelihood to how exploitable or vulnerable the system may be, rather than the intent of the attacker.

Cyber-physical approaches combine the assessment of vulnerability with efforts to understand consequence. Some authors tie together enterprise and control system networks and look at the vulnerabilities, others look strictly at the vulnerabilities of the control system networks themselves. Because consequence is non-deterministic, it is not always clear how a particular compromise may play out in the controlled system. Modeling of the coupled systems is used for better understanding the consequences to determine which portions of the system need to be protected and which vulnerabilities need to be addressed.

The mission assurance space focuses on consequence to the mission that the information technology (IT) system is supporting. Tying a cyber incident to an impact on mission allows the discussion of risk to go beyond network defense and vulnerability identification to exploration of ways in which consequences can be mitigated. Mitigation options can include the creation of situations in which system compromise presents less of a critical incident from the mission accomplishment perspective.

1.2. Organization of document

This document summarizes the findings for the three different areas found in the literature review: network security, cyber-physical, and mission assurance. One section is dedicated to each area and summarizes the body of work reviewed and the identification of any assumptions inherent in the viewpoints expressed. The final section summarizes the findings and discusses implications for securing enterprise networks. The section also includes a listing of techniques that can be adopted from the different areas and tied together to achieve a more comprehensive risk analysis. Finally, all of the reviewed articles and their abstracts are presented in the bibliography (Appendix A).

2. NETWORK SECURITY

Network security uses a variety of modeling approaches that range in level of detail from packet-based simulations of network traffic to network graphs. The focus of the articles in this space is a better understanding of the network and methods to provide better security.

Modeling techniques are employed to help secure networks to avoid disrupting an operational system whose goal may be availability. Techniques to explore vulnerabilities may break existing systems and deem them unstable, modeling eliminates the risk of system disruption while examining vulnerabilities.

Modeling can also provide a unique look into the graph structure of networks and differing approaches to examining networks, whether the focus is on end points or on network traffic. NetFlow[1] data or packet capture can be used to examine network traffic. Networks can be modeled based on the protocols used or the privileges invoked when data traverses a particular path. This becomes crucial in terms of knowing how to restrict the traversal of data or where to restrict users from having certain privileges. Modeling based on protocols or privileges provides insight into unnecessary protocols allowed on the networks and how the systems respond to malicious external requests.

The important question for network modeling in the context of network security is the level of granularity of the model. For information networks there are several granularity levels possible. The primary approach for security evaluations in the reviewed articles is some form of network or attack graphs such as in Hong (2014) or Kotenko (2013). Another approach is to model at the level of computers and network devices (Nicol, 2003). This can be useful for simulating alerts from intrusion detection systems in order to develop situational awareness and threat assessment tools. Another approach is simulating computer network traffic at the packet level (Lee, 2004). Such simulations visualize the effects of an attack on each layer of a network stack and on applications. While not in the scope of this literature review, modeling is also used to look at attacker and defender behavior such as in Wang (2009) who uses it to find an equilibrium for network confidentiality and integrity.

2.1. Network and Attack Graphs

Network graphs are the starting point for many of the analyses in the reviewed articles. A graph is a mathematical object consisting of a set of vertices and edges. An edge connects two vertices or the same vertex. A network graph can be developed to capture a variety of connections. For example, it may consist of nodes representing computer systems with either logical or physical links as edges. Alternately, computer system services may be the nodes, with edges mapping to the device that hosts those services. In Hong (2014), network graphs are used to look at connectivity of nodes within the network to gauge the importance of any given node and help prioritize vulnerabilities to patch. Yusuf (2016) parameterizes network graphs to better account for changes in networks and network configurations and to explore how metrics change as the status of vulnerabilities change. Rasche (2007) moves graphs down to the level of detail of physical and logical network connectivity as well as hardware and software characteristics,

[1] NetFlow tallies packets and bytes for flows that have the same source and destination IP address and ports, protocol interface and class of service. http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html, accessed June 2017.

allowing linking of protection mechanisms such as firewalls to networks and hosts. The architectural model of the network is then used to verify implementation of security requirements. Soule (2015) also employs an extremely detailed model of the relevant system and applies automated methods to the description of cyber systems, defenses, attacks, missions, and metrics to attempt to minimize cyber attack surfaces such as pathways that provide access. Creese (2013) combines network graphs with business process models to create a visualization framework that shows attacks and their potential impacts on business processes. This framework requires the characterization of the links between network components and business processes.

A graph called an "attack graph" is also frequently employed in the network security space. Attack graphs show the paths an attacker can use to gain access to a targeted network or achieve a particular goal on a system or network (for example, gaining access to what should be a protected database and downloading the data). The vertices of an attack graph can be divided into three partitions: starting places, "flags" or goals, and intermediate steps. They may contain alternative steps that could be taken to achieve a particular goal which could range from direct compromise of system elements (run a Server Message Block protocol (SMB) exploit against a vulnerable machine), to other methods of achieving the goal (impersonate a vendor to gain physical access to a machine).

Abraham, in a series of articles published in 2015, uses attack graphs as an analytic tool, expanding attack graphs to include how vulnerabilities age, and how they are discovered to determine how susceptible those vulnerabilities are to exploitation.

Several authors extend the use of attack graphs as analytic tools into the space of automatic generation. Kotenko (2013) develops a framework for attack graph generation and impact assessment based on host vulnerability, attack probability, adversary ability, and estimated system response. Holm (2015) creates a method for directed attack graph generation based on assets, their relationships, attacks, and defenses. Välja (2015) extends the work of Holm to include availability and interoperability as part of the analysis. The model also includes reachability of a particular node relative to attacker skill. Xie (2010) provides an extension to attack graphs to capture uncertainty in attack structure, attacker actions and the corresponding alerts. While the uncertainty does not go as far as to model at the packet level, it moves attack graph analysis closer to packet-level network security analysis.

Rahman (2013) creates a qualitative risk analysis model that accounts for reachability, to include reachability through intermediate hosts. Vulnerability, host assets, and network topology make up the network model. Paths are traced through the network to determine reachability. The network model and the security requirements are developed into a constraint-satisfaction problem. The results are used to determine necessary firewall policies and host placements.

Henshel (2016) develops a risk-based approach to cybersecurity decision making that has similarities to attack graphs but uses them as a form of risk and mitigation option assessment. The approach provides a set of alternative actions and associated cost-benefit tradeoffs. The model captures system and human states and calculates risk for each task based on known and predicted threats (for example, by capturing both user access permissions for a particular resource on a system, and the risks associated with the geographic location of that user). Risk variables are chosen based on the components that comprise the system. Experts are used to determine the relevant assessment and measurement variables. Probabilistic network analysis is then used to compute the risk.

Red teams may employ attack graphs as part of the security analysis of a system. They provide the system owner with information on vulnerabilities, impact and, based on the difficulties that the team encountered, the likelihood of successful attack. An attack graph has some relation to the network that is the focus of the red team evaluation. However, the purpose of an attack graph is not to reveal the network to be attacked but rather to help the red team visualize their work. Conceptually, the team members start at any given vertex and then try to advance to adjacent vertices. One of the intermediate steps might be labeled, "Dumpster dive to obtain list of user names." Another intermediate step might be labeled, "Social engineer to obtain list of user names." If the team gets such a list either by dumpster diving or social engineering, then the team might encounter a subsequent intermediate step labeled, "Find personal information" which would lead to "Prepare phishing attack." A flag vertex might be labeled "Send forged e-mail to CIO." As the red team proceeds they might choose to reflect in the graph what they have learned, possibly modifying it. Attack graphs thus assist a red team in both planning and execution as well as, when the exercise is over, explaining to the client what the team tried, what they discovered along the way, and what worked and what did not. Figure 1 shows a simple attack graph and the associated network graph. Several authors such as Applebaum (2016) provide techniques to automate red team activities and generate attack graphs.

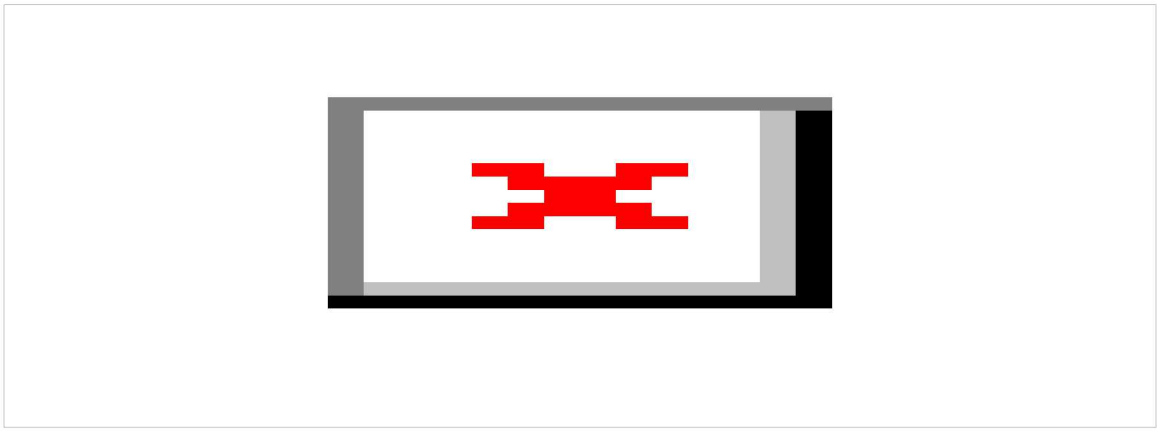

Figure 1. Simple network and attack graphs[2]

2.2. Packet-level Modeling

Packet-level models in the network security space focus on better characterizing attacks so that defenders can create better defense techniques such as improved firewall rules and intrusion detection algorithms. These models can also be used to enhance network analysis.

To use packet-level models for network analysis, there is often a need to run multiple simulations and have those simulations run in faster than normal clock time for network activity, for instance, when a simulation is used to help defend against an attack. Working through the consequences of contemplated defensive actions helps to identify feasible (or even optimal) decisions. Nicol (2003) looks at packet-level events in faster than real-time by using model

[2] This figure appeared as Figure 1 of Lippmann et al., "Evaluating and Strengthening Enterprise Network Security Using Attack Graphs," ESC-TR-2005-064, Lincoln Laboratory, https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/0507_Lippmann.pdf, accessed July 2017.

abstraction. The paper provides simple analytic methods to help achieve that abstraction and faster run times.

Lee (2004) goes even further, modeling cyber attacks within an operating system to include packets and system level events. In contrast to the cause and effect model of threats, attacks, and defenses developed by Cohen (1999), the authors use a discrete event simulator to reproduce detailed cyber attack behavior. The detailed cyber attack information is then used to explore defense strategies.

Constantini (2007) describes a simulation capability for the synthetic generation of networks, attacks, and intrusion detection alerts to assist in developing tools that can detect and act against attacks. Kuhl (2007) discusses Constantini's simulation capability with specific regard to generating cyber attack scenarios, ground truth information, and information fusion to look at ground truth versus the full set of intrusion detection alerts.

García-Teodoro (2009) provides a survey of research into intrusion detection using anomalies rather than attack signatures. Anomaly detection looks for unusual behavior potentially revealing attacks that have not yet been seen and characterized. Much of the research discussed in this article relies on modeling of traffic at the packet level to develop the appropriate algorithms.

Lee-Urban (2016) models the propagation of malware across networks at two different levels of fidelity which are built in a discrete event simulator. One is a pure simulation at the macro level which supports simulation of protocol-level events where nodes represent simulated hosts. The other uses nodes that emulate the behavior of computer systems and can include real hardware and real software. The authors provide examples of evaluation of malware in both levels of fidelity.

2.3. Summary

The majority of the modeling approaches discussed in this section make several key assumptions:

1. A diagram of the network exists. It may be an architectural diagram of the system as designed, or the current system as it existed the last time someone looked. At a minimum the diagram would represent the devices on the network and some concept of connectivity between them. In the case of a red team assessment, the team may be given this graph or asked to create it, depending on the style of assessment being conducted. None of the articles discuss creation of network diagrams, nor did a search of associated terms discover articles relating to the creation of network diagrams.
2. Critical system elements or functions have been identified. This may be a system that contains information that needs to be protected (confidentiality or integrity), or a network or device that always needs to be available (availability). Before network modeling for security begins, the decision has already been made that these particular elements need to be protected.
3. Consequence is assumed. Network security approaches assume that loss or compromise of the critical functions or elements of the system need to be controlled or avoided. This leads to the focus on network defense rather than on exploration of consequence, so consequence is not directly modeled in the majority of approaches.

The exception to this among articles reviewed for analysis of the network security space is Creese (2013), though this work focuses on visualization of attacks and impacts rather than directly on securing the network.

This page intentionally left blank.

3. CYBER-PHYSICAL SYSTEMS

Another large grouping of articles found in this literature review of cyber and modeling research examines the cyber security of cyber-physical systems. Cyber-physical systems are systems that integrate physical processes and computational components.[3] Drias (2015) provides an overview of industrial control systems' architectures and protocols. As expected, a large number of these are associated with the power grid, either in relation to the incorporation of smart grid, or studies of electric power Supervisory Control and Data Acquisition (SCADA). Modeling within the cyber-physical realm uses some of the methods found in network security but more deeply investigates consequence assessment, tying the cyber system to controlled physical assets. Much of the detailed modeling addresses the physical power grid rather than the control system.

3.1. General Cyber-Physical Methods

The articles discussed below do not explore any specific system, but leverage methods in the network security realm that were discussed previously, including attack graphs and packet-based models. The focus is in broadening the network security related work to apply, more specifically, to control systems.

With the increased industrial system reliance on information and communication technology as a motivator, Masera (2006) discusses bringing the concept of an information asset (e.g., commands sent to control systems, data in a databases) into risk assessment. Typical risk frameworks begin with descriptions of some combination of services, components, assets, and relationships. The authors create a characterization of information assets and discuss confidentiality, integrity, and availability as security properties of those assets. The paper then formalizes the representation of the systems at different levels through which information assets flow.

Ekstedt (2009) begins to consider the control system within the broader information technology context, but does not move into the consequence space. The authors develop a method for cyber security analysis of the control system along with its surrounding organizational environment. The method is similar to the attack graphs coupled with security information, uncertainty, and countermeasures discussed in the network security section of this document. By incorporating the control system's IT and organizational environment, this method attempts to provide a more holistic understanding. The model is designed to allow decision makers with limited knowledge of control systems to make better decisions.

Also not addressing consequence, Ma (2013) uses a vulnerability-centered approach to look at cyber risks. The model focuses on hosts and their connectivity. Vulnerabilities are mapped as preconditions and effects. Preconditions are the conditions that must be met for an attack to succeed (for example, the presence of a vulnerability, the attacker's level of privilege, and knowledge of network connections). Attack paths through the system are identified and then can be used to control or mitigate risk.

While node importance is discussed in Wu (2015), there is little discussion of how that importance is developed. Wu ties risks to vulnerability in the cyber-physical system, specifically of attacked hosts, and to that host's importance in the system. The risk calculation for the host is based on attack severity, the probability of success, and the consequence. The overall risk for the

[3] National Institute of Standards and Technology, https://www.nist.gov/el/cyber-physical-systems, accessed June 2017.

system is the host's risk coupled with the importance of that host. In the case presented, hosts are within the control system and could range from sensors to controllers. Host importance is tied to economic loss, casualties, environmental damage, and repair costs of the controlled physical asset.

Orojloo et al. (2014) consider their primary contribution to the cyber-physical security analysis area the inclusion of cyber attacks that can lead to physical damage and factors that impact an attacker's decision-making. Their model also includes attacker and system behavior over time. The proposed approach is a state-based stochastic model that can be solved to quantify the security measures of the system, such as mean time to security failure (MTTSF), steady-state security, and steady-state physical availability from a cyber attacker's point of view. Components are categorized with respect to their susceptibilities to cyber attacks on availability, confidentiality, and integrity. Attack paths are then developed which include states and the necessary actions to transition between states. The model assumes that components with higher interconnectedness and interdependency are more likely to be attacked. Beyond interconnectedness there is no additional metric for the potential value of a component, but value is considered as an attractiveness factor of a component to an attacker.

In addition to providing an overview of cyber-physical systems and protocols, Drias (2015) discusses security concerns for industrial control systems. Similar to Orojloo (2014), attacks are categorized into those impacting availability, confidentiality, and integrity of the industrial control system. The authors observe that IT solutions are currently being applied in the control system despite not being specifically designed for that system. The work calls for tailored solutions specific to industrial control systems.

Wan (2015) creates a security-aware functional model that couples the control system with the physical system and adds elements to incorporate cyber attacks. The goal is a simulation model that can be used in early stages of design to identify flaws and improve operational integrity. The functional model includes mathematical formulations for the physical processes within the system and the information flow from the controller to those physical components. Several mathematical attack models are then created to manipulate the information flow. These include denial of service, signal noise, and replay attacks. The functional model is demonstrated on an automotive system as a test example.

McDonald (2010) develops a modeling and simulation environment to investigate control systems at the protocol level and the associated processes being controlled. The environment is able to replicate control system protocols at a level of fidelity that allows for the inclusion of real components within the environment. It is designed to allow researchers to explore, design and test mitigations on a modeled system as though it were the real thing.

3.2. Electric Power SCADA

The largest cyber security modeling body of work in cyber-physical systems focuses on the electric power sector. Within the area of electric power cybersecurity, Ten (2010) proposes a security framework for SCADA consisting of four major components: 1) real-time monitoring; 2) anomaly detection; 3) impact analysis; and 4) mitigation strategies. While calling for more detailed techniques in each of the four areas, the authors develop a simplified method for utilizing an attack tree to evaluate cybersecurity of a power control system as a proof of concept.

Palensky (2014) explores the scalability issues of time-based and discrete event-based simulations for cyber-physical energy systems. The paper describes the four domains that need to be addressed in the power grid hybrid system: 1) models of the physical system that are continuous; 2) models of information technology that are discrete and event-based; 3) game theoretic models for individual agents (customers, market players); and 4) additional aggregated and statistical models that may feed individual elements (weather, generalized characteristics, etc.). The paper then documents creation of a scalable test model of a hybrid system in a continuous construct and in a discrete-event construct to look at scalability. The authors discovered that discrete event models had better runtime performance and that the continuous time approach is well-suited to scenarios with more sophisticated and complex physical models. The authors believe the advantages are complementary and call for a hybrid approach to modeling complex energy systems.

Pasqualetti (2011) presents a framework and monitoring procedures to detect and identify network component malfunctions or measurement corruptions in the power grid caused by an adversary. The detection process exploits the dynamic characteristics of the grid. The authors conduct their work on a model of the grid itself, rather than on the associated control system networks to develop their framework, with the assumption that the control system network is monitoring the appropriate outputs.

Vellaithurai (2015) develops a risk management technique that calculates (in near-real time) cyber-physical security indices to measure the security level of the underlying cyber-physical system. The proposed approach requires instrumentation of the control system hosts to monitor information flows among system assets. Using a list of mission-critical assets provided by the administrator, the technique constructs the normal communication patterns from the sensor inputs and generates a dependency graph that can be used for security analysis. The power grid is modeled as a graph to explore potential contingencies and severity of impact. The illustration of the method includes the control system network, a power relay switch, and the corporate network.

Cheh (2015) creates a cyber-physical topology language to describe a system and its associated security state with the goal of using physical and security sensor information to help describe that state. Weaver (2016) expands on Cheh's work and creates an 8-substation cyber-physical reference model using the cyber-physical topology language that includes both the physical system and the control network. The goal of the model is to better understand the interconnectedness between electrical and cyber infrastructures so that system reliability can be maintained. This work illustrates some of the difficulty in obtaining information for accurate network topology creation. Development of Weaver's 8-substation cyber-physical reference model required visits and interactions with utilities.

Zhang (2015) develops and uses attack graphs incorporating probability to look at intervals of successful attacks (mean time to compromise) for various networks associated with the power grid. The networks include the corporate network, primary and backup control center networks, and 24 substation networks (with varying degrees of automation). The IEEE reliability test system 79 is used to evaluate load loss probability due to the attacks. The work shows that as the mean time to compromise becomes shorter the reliability of the power grid decreases. Shorter mean times to compromise result from increasing skill levels of attackers coupled with increased probability of a successful attack sequence to achieve a particular goal.

Davis (2015) develops a framework to assess power system reliability due to dependencies on and weaknesses in the cyber infrastructure. The algorithm computes risk metrics based on the physical and cyber components. The power system model uses a state estimator and a full breaker-level topology to calculate system state. The cyber topology is a logical network incorporating rules about which hosts on a network are able to communicate. The framework uses attack graphs to determine which cyber intrusions could lead to line contingencies. Probability of success and the severity of the power system impact resulting from the compromise of the control system component associated with a particular element are part of the reward function for the attacker.

Zhi (2011) describes work to simulate electric power infrastructure networks using a suite of simulation approaches including: (1) network topology generation models, (2) agent-based physical and control system simulation models, (3) associated dependent models, and (4) cascading failure propagation models. The authors abstract the power system into a series of nodes and edges to connect control system elements to physical grid elements. On the physical side the model uses optimal power flow calculations to examine impacts and also incorporates regional parameters to generate load. The details of the control system side are not well described aside from specifying an agent-based model.

Liu (2017) explores the impact of physical protection systems, specifically bus and transmission line protection systems, on cyber security risks. The study uses a Monte Carlo simulation to randomly modify parameters and then analyze grid behavior. First connectivity is checked and if it is maintained, a power flow solution is performed to check for violations. If the power flow does not solve, a load curtailment strategy is performed until a solution is feasible. Once a solution is reached, the risk assessment is run. Risk is measured by the expected load curtailment.

Kalluri (2016) explores denial of service attacks on SCADA components to determine the associated response time of components in the SCADA network. The results indicate that denial of service attacks of various types can disrupt communications between components of the SCADA system. The work does not go into a broader model of either the control system or the power grid.

3.3. Smart Grid

Several articles found in the literature review explore the implications of smart grid on cyber security modeling and grid security. Sou (2013) looks at false data attacks in electric power networks containing smart grid components. The work develops potential mathematical solutions to create a security index that identifies the minimum number of measurements an attacker needs to compromise in order for an attack on a specific measurement to be undetected.

Mo (2012) presents theoretic approaches and examples for smart grid security accounting for the cyber and physical aspects of the system. The authors break down the portions of the grid into generation, transmission, distribution, and consumption and explore the related information security requirements. They also provide a discussion of cyber and physical consequences of various types of attacks and discuss potential countermeasures. The paper calls for additional work in using information security and system-theory-based security to secure cyber-physical systems.

Chen (2012) explores vulnerability, data injection, and intentional attacks and their countermeasures. Intentional attacks are those that use knowledge of the structure of the network to disrupt network operations and are the detailed focus of the work. Similar to Wang (2009), a game theoretic approach is used to look at attacker and defender behavior. The outcome of the game equilibrium is considered the robustness of the network at the stable state.

Jauhar (2015) models one of the failures developed by a consortium of grid operators, security consultants, and regulators. The failure scenario describes an undesirable cyber incident, its impact, and the vulnerabilities and potential mitigations. The model generates what the authors term a security-argument graph that includes system components, the workflow they implement, and a description of the skills and resources of the attacker. The model uses extension templates to capture probabilities for successfully exploiting vulnerabilities, thus creating an attack graph that includes probabilities. The extension templates are created and then reused, since many of the studied failure scenarios share similar types of attacks. The calculation of these probabilities across the graph to the goal node is the quantitative risk metric.

3.4. Other application spaces

Kiesling (2016) develops a model-based approach to assess cyber security risks in the global air transport system. The method begins with an architecture model of the European Air Traffic Management Architecture. The approach consists of a model of the attack, a model of the target of the attack, and an impact model. The attack model is probabilistic and consists of the actor, the resources of the actor, and the tactics, techniques, and procedures that can be used to achieve the intended effects. The target model is a subset of the architecture model of the system. The impact model relates the elements of the architecture to pre-assessed impacts based on a specific degradation of that element.

Easwaran (2017) develops attack sequence diagrams for use in design of safety critical systems such as avionics and automotive controls. Attack sequence diagrams are an extension of sequence diagrams which model resource request, allocation, and temporal properties. The work focuses on the importance of deadlines related to these systems and considers attacks that disrupt those deadlines. The goal is to use the diagrams to help generate potential attack paths in the design phase and explore the trade-offs for implementation of countermeasures within the designs. The attack sequence diagrams resemble attack graphs but also link in the timing needs associated with the physical system.

Yoneda (2015) looks at cyber and physical threats within an office with both information and physical security systems in combination. A list of risks was developed and classified into four categories in a matrix based on their risk probability and impact, each from low to high: risk transference, risk mitigation, risk acceptance, and risk avoidance. Using the resulting risk matrix, countermeasures were proposed. The authors then quantify risk using the value of the asset, the value of the threat, and the value of the vulnerability. Asset value is approximated by risk impact, threat value is approximated by risk probability, and the value of the vulnerability is determined by the quadrant of the category in the matrix, with one being the lower left, and the highest value, 3, in the upper right.

Rodríguez-Mota (2016) focuses on the Internet of Things (IoT) and presents a method to create an IoT visual system representation to help identify new attack surfaces or attack vectors in the existing infrastructure. The visualization incorporates communication patterns, infrastructure

topology, and device capabilities. The example provided is a study of application permissions in Android and their related risks.

3.5. Summary

One of the articles identified in our review was a more narrowly-scoped survey of research on model-based security engineering for cyber-physical systems. Nguyen (2016) finds that most studies focus on general security analyses based on threat, attacks, and vulnerabilities rather than on security concerns such as confidentiality, integrity, and availability. The security concerns are addressed implicitly rather than explicitly (e.g., discussions of host compromise, or access to data as attacker goal examples). Our findings in both the network security and cyber-physical security areas match the study except for Orojloo (2014), which does address availability, confidentiality, and integrity as attacker objectives, and Drias (2015), which discusses security concerns.

In contrast with Nguyen (2016), we found several studies that include uncertainty in the form of the probability of attack success in the cyber-physical literature. The articles that deal with uncertainty employ attack graphs and other methods commonly used in the network security literature and extend them into the cyber-physical space.

Much of the cyber-physical modeling involves the power grid and more detailed models of the grid itself rather than of the control network. Studies exploring the control network tend to use attack graphs and some form of probabilistic assessment, similar to the network security spaces. Those probabilities are then coupled with impact on the grid of component compromise. Impact is either calculated through detailed power flow models or through some measure of importance of that component in overall operations.

Significant work exists in attempts to tie attacks on the control network to detailed consequence on the power grid. The work tends to assume that if a control system component is compromised, its controlled device on the grid is negatively impacted (e.g., a breaker trip). Detailed power flow modeling is done in many cases to determine what that may mean to overall grid performance.

4. MISSION ASSURANCE

Mission assurance is a field in which cyber systems are treated as enabling a particular function. The focus of the work is to determine impact on a mission or process due to the loss of supporting IT infrastructure and to try to ensure mission function. Musman et al. (2009, 2011b, 2015, 2016) published a series of articles exploring how to relate cyber attacks to impacts on missions. Similar to Creese (2013), Musman (2009) discusses linking cyber resources to business processes. However, unlike Creese, the goal of the work is to go beyond visualization to create a model that would allow a cyber attack to be an input to a calculation of metrics for mission success. The desire to understand timing both of the mission elements and in terms of the duration of the effects of the cyber attack within the model are reminiscent of Easwaran (2017) in the cyber-physical realm, though this work predates Easwaran by many years.

4.1. Literature

Musman (2009) develops a set of modeling requirements for the mission model and categorical descriptions of cyber attack effects. The mission elements are documented in the Business Process Model Notation, and the IT portions are populated from network diagrams and detailed information about software applications and anything within them that may affect the workflow. In Musman (2011b) the authors describe the development of the model requirements into a combination of commercial-off-the-shelf tools and describe in more detail the translation of the six cyber-attack-effect categories into impacts. Musman (2015) describes the redevelopment of that tool into custom software for better functionality and a focus on cyber processes, resources, and cyber incident effects.

Musman (2011a) expands on the work in process modeling to use the developed models to determine the system crown jewels, examine their susceptibility to different attack effects, and evaluate mitigation techniques. The crown jewels in this context are the cyber elements that are most critical to the accomplishment of an organization's mission. The work builds on Hastings (2009). The analysis can show which IT assets are mission critical and which are most important to each mission activity.

Monteiro (2016) applies the principles in papers by Musman (2009, 2011a, 2011b) to civilian air infrastructure. Rather than simply using network connectivity, the authors incorporate simulation environments for both wireless communications and network protocols into their framework. The authors also incorporate models of the air traffic control system, aircraft in flight, and communications between the pilot and the controller. Although this article explicitly references the Musman, et al. body of work as background, it could also be categorized in the cyber-physical space.

In Musman (2016), the authors extend the process modeling work by applying an attacker and defender game theoretic approach to one of the previously developed workflows. This is similar to the approach in Wang (2009) and Chen (2012), however the probabilistic attacker model also accounts for the possibility that the attacker has compromised a similar component already. The threat model is somewhat less detailed than in prior work since it does not rely on a detailed attack graph, using instead a series of conditions (such as does the attacker have to cross a network boundary or is the compromised resource a server). The model is then used to assess the utility of various defender actions and determine system resilience in the face of an attack.

Sun (2016) explores the impact on assets of cyber attack and calculates the operational capacity of an asset after an attack. That operational impact is then rolled into an impact on services that asset helps to provide and, ultimately, is elevated further to impacts to the mission. This goes beyond the impact work by Musman (2011b) by defining an explicit service layer and looking at degraded capacity.

Buchanan (2012) develops a proof of concept to automate the creation of the mapping between cyber assets, missions, users, and cyber capabilities based on information already available on the network. A capability is the ability to perform a particular action; it provides the link between users, missions, and assets. The work maps dependency relationships with three properties to capture the criticality of the dependency: uses, depends on, and requires. The relationships are inferred based on criteria related to network traffic between hosts. In this way, the work attempts to get at which assets are actually used in a particular mission and capture the potential for that to change over time.

In Llansó (2012), the authors describe a software platform for studying the link between cyber attacks and the impacts on operational missions. The system automates attack path generation and provides a prioritized list of potential security controls based on historic attack information. The authors mention automated architecture detection from the live network as a potential direction for future work.

Llansó (2014) moves the earlier work into the space of computing risk by using the level of effort to carry out an attack and the level of impact on the mission due to the attack. A vulnerability profile of each node is developed, ideally using scanning and penetration testing, and assigned a level of effort score for breaches relating to confidentiality, integrity, availability, and transit. Transit breaches are potential pivot points in the cyber architecture. Scores are from 1 to 10, with 10 being the most capable attacker. The system then computes the lowest level of effort attack paths. Mission experts are used to identify measures of effectiveness and the logic that links IT elements to the measures of effectiveness. A risk matrix is then used to compare the various attacks and help decide on mitigations.

Llansó (2015) expands the prior method to estimate attack level of effort beyond subject matter expert input. The developed approach is heuristics-based and accounts for attacker capabilities.

Similar to other work in the space, Jakobson (2011) develops a method to characterize the impacts of cyber attacks on network assets, services, and missions. The method starts with assessment of the direct impact of the cyber attack, then propagates that impact through the logical dependencies. The operational capacity is calculated for assets and services that are on the path of cyber attack impact propagation based on those dependencies. Finally the mission impact is calculated based on the connections between the cyber services and the mission. The method also incorporates time-dependent mission tasks, missions, and services.

Jakobson (2013) describes the architectural principles of achieving cyber-attack-resilient missions. These include mission-centric cyber security, adaptation, synergistic command and control, and cyber security management. The authors defined three key components of cyber-attack-resilient missions: 1) predict plausible impact of attacks before they occur, 2) survive through adaptation and graceful degradation during the attack, and 3) recover operational capabilities after the attack. They define three conceptual components to the approach: cyber terrain, or IT infrastructure modeling; mission task flows; and impact dependency graphs to

connect the two. The work lays out concepts and potential approaches, but further work is required to turn the concepts into operational tools.

Pritchett (2012) reviews the 24th Air Force cyber mission assurance guidance, best practices from commercial, government, and military, and lessons learned from the operational environment. The goal is to provide a guide for determining and prioritizing mission critical elements linked to cyber critical assets. The work also discusses reducing uncertainty in the space by conducting exercises. A collection of tools and techniques to collect data related to the missions and the mapping to cyber assets is presented. The author also discusses prioritizing the missions from most to least critical to determine where to begin the process.

Jabbour (2011) decomposes missions into cyber processes based on intelligent systems. Intelligent systems are computers executing a sequence of instructions. Missions are characterized based on the security attributes of the cyber processes. The mission assurance process is composed of: prioritization of missions, mapping, vulnerability assessment, and mitigation. Red teaming is also listed as an optional step.

Guariniello (2014) modifies a functional dependency analysis tool to look at system-of-system operational and communication architectures. The goal of the work is to compare different architectures in terms of reliability and robustness under attack. The work focuses on the interdependency between systems to look at the behavior of the whole system-of-systems under attack. This work does not explicitly look at mission assurance but at system survivability.

Ormrod (2015) develops an ontology to explore the system-of-system effects of a cyber attack on an organization or military unit. The ontology consists of four different domains that are connected together: physical, virtual, conceptual, and event. The physical domain represents physical assets. The virtual domain includes the logical and cyber persona layers (for example, an email message, software vulnerability, or user account). It also includes a representation of a user. The conceptual domain includes logical groupings as organizations and processes to include missions. The event domain provides the interactions between physical and virtual, and allows the impact of an event in one domain to propagate across others. The domains are linked through common objects, or, where that is not possible, an inference layer that can propagate effects between domains. The authors discuss developing the ontology into a model as future work.

Naumov (2016) develops high-level causal relationships of both internal and external cyber-related risks. These relationships are then used to assess the high-level dynamics of the system. The goal is to be able to assess how these relationships and dynamics change an enterprise's cyber risks over time. For example, trends towards an increased digital footprint, or more highly integrated partners and clients, would increase potential risk exposure. This capability would allow companies to better understand how changes could impact cyber-related risks.

Naudet (2016) explores risk management in networked enterprises. The goal is to account for interaction of organizations and the environments they sit within in enterprise risk management. The elements included in the model are assets and the criteria which guarantee their security; risk as the combination of an event and the negative impact it has on an asset; and risk treatment. Assets are things that have value to the organization and are necessary for achieving objectives. These can be business or IT assets. Events combine vulnerabilities and potential attacks and methods. Risk treatment is a decision to treat an identified risk combined with security requirements and controls to improve security. This model is extended to look at each system

coupled with its environment and the interaction between those systems. This allows for the linking of assets across organizations and for risks to propagate.

4.2. Summary

Keith Rhodes, the Government Accountability Office's first chief technologist, argues in a Washington Technology opinion piece published in 2010 that cybersecurity needs to be about mission assurance.[4] Given that cyber security perimeter defenses can never be perfect, cyber risk needs to account for the dependencies between the cyber system and the overall mission that cyber system is helping to achieve. The articles in the mission assurance space tie cyber assets into some form of consequence on the larger system. This is very similar to risk analysis in the cyber-physical space, though mission assurance also tends to explore mitigations. Very few of the network security articles discuss system consequence.

Many of the techniques used in mission assurance are similar to the cyber security aspects of network security and the goal of determining the impact of cyber-physical related articles. Similar to cyber-physical, the cyber system in many cases is not simulated in great detail, while significant effort is put into exploring the impact portion. Monteiro (2016) goes the farthest in the space to tie together detailed simulations of both the cyber aspects and the system aspects.

Timing of incidents and how they propagate with respect to time in the execution of the mission are a stronger focus in this space. Only Easwaran (2017) was found to have started to focus on timing and deadlines for safety-critical systems. The mission assurance space focuses more strongly than cyber-physical on impacts to system resilience and the ability to still perform the mission.

[4] K. Rhodes, 2010. Cybersecurity must start with mission assurance, Washington Technology, Jan 15, 2010, http://washingtontechnology.com/Articles/2010/01/13/Predict-globally-protect-locally.aspx?s=wtdaily_190110&Page=1, accessed June 2017.

5. IMPLICATIONS FOR MANAGING ENTERPRISE CYBER RISK

The goal of this work was to explore the research in areas relating to modeling of cyber risk, identify the trends, and provide recommendations on literature results that may be applicable to managing cyber risk in enterprise networks that go beyond the network security regime. The review found three different areas in which modeling of cyber risk is discussed: network security, cyber-physical, and mission assurance. Some of the methods used to explore risk cross areas. For example, the cyber-physical realm has adopted the probabilistic attack graph approach used in network security to think through vulnerabilities and the difficulty of executing a particular attack. Cyber-physical investigations into risk go further into consequence assessment than many of the articles in the network security space.

Risk is a function of threat, vulnerability, and consequence. However, in the majority of the reviewed network security literature, the focus is analysis of vulnerability and threat in combination. Threat in the form of intent is not considered. Threat is explored through examining the capability of the attacker, and making network asset exploitation as difficult as possible. To achieve this, a combination of asset-based security and network security practices are used. These include better intrusion detection techniques and use of monitoring and countermeasures. For vulnerability analysis, the cyber-physical realm has adopted many of the practices used in the network security space such as attack graphs and analysis of network topologies. While all of the articles recognize that having an accurate network topology is critically important to risk management, none discuss how to obtain such a topology.

The network security space is relatively silent on the notion of consequence. However, both the cyber-physical and mission assurance spaces focus on tying cyber events to some form of impact. Detailed cyber-physical analysis in the power grid examines consequence by looking at how compromise of a cyber component may cause a grid element to fail, and tracing that failure through to the impact on power flow in the grid. More aggregate analyses, including the process-based studies in mission assurance and a small number of articles in network security, look at how loss of a cyber asset may affect business or mission processes.

Enterprises could better manage cyber risk by adopting some of the approaches used in mission assurance and cyber-physical analyses to link cyber assets to business processes. Functional process diagrams can be used to tie functional elements to cyber systems and assets. With that information, risk managers can make better decisions about what portions of the network are most critical to business functions. In addition, tying risk to impacts on business processes allows risk managers to move beyond defensive measures into more proactive measures that could help mitigate consequence and ensure business process survivability. Rather than prioritizing only the criticality of cyber assets, risk managers can weigh costs and benefits to prioritize resources by mission and the assets and systems tied to that mission.

From the literature review, the necessary components to manage cyber risk and prioritize resources for protection or mitigation are as follows:

1. Control Vulnerability
    a. Characterize the network – it is difficult to manage unknown elements. Therefore, creation of a network graph is required. A comprehensive graph should include the following:
        i. Hardware and software assets

        ii. Connectivity between assets
        iii. Asset configuration and vulnerabilities
    b. Attack graphs – attack graphs start with network graphs and provide a method for exploring potential network attacks and their prevention. They can also include the level of capability of an adversary to help answer the question of "how hard do I have to make it to successfully attack my network given the adversary I am concerned about?"
    c. Traffic analysis – once a map exists, traffic analysis on the network can assist with detecting and preventing malicious behavior.
        i. Intrusion detection
        ii. Intrusion prevention
2. Understand consequence – consequence is determined by mapping cyber networks and assets to enterprise missions or functional processes. Risk managers must answer the following questions:
    a. What are the key enterprise processes or missions?
    b. Which cyber assets or systems support those processes or missions?
    c. What happens when those cyber assets or systems are disrupted or manipulated, or when information is lost? (This accounts for availability, integrity, and confidentiality as a requirement of the mission or process.)

To manage risk across large enterprises, the functional process diagrams must include processes that cross divisional boundaries in an organization. Otherwise, attempts to prioritize resources to manage cyber risks will only capture individual division priorities and not speak to overarching missions. This can be achieved by divisions creating functional process diagrams where elements that enter and leave the process are treated as inputs from and outputs to other divisions. Integrating the diagrams from each division would create a holistic picture.

An enterprise may evaluate the level of integration it has with its partners from a cyber exposure and risk perspective, but inputs or outputs to those partners are external to the process. Risk exposure related to cloud resources can also be addressed in this manner. Once the risk of putting process elements or processes into the cloud has been examined and accepted, cloud resources can become inputs and outputs that are external to the process.

The complete picture of the cyber system coupled with its processes allows a risk manager to prioritize cyber systems and assets based on the missions they support, and determine which cyber components are most critical to the execution of those missions. The risk manager can also look at the cost-benefit tradeoffs of either further securing those elements or creating mitigations so consequence is reduced. This allows the risk manager to assume that their defenses are not (and never will be) perfect, and look for additional options that provide benefit in terms of the organization accomplishing its mission under the conditions of a successful attack.

APPENDIX A: BIBLIOGRAPHY

In the bibliography that follows each citation is followed by a link to the paper, followed by the abstract. The articles are categorized by references related to network security, cyber physical systems, and mission assurance.

Network Security

S. Abraham and S. Nair, "Exploitability analysis using predictive cybersecurity framework," *2015 IEEE 2nd International Conference on Cybernetics (CYBCONF)*, Gdynia, 2015, pp. 317-323.

http://ieeexplore.ieee.org/document/7175953/

Managing Security is a complex process and existing research in the field of cybersecurity metrics provide limited insight into understanding the impact attacks have on the overall security goals of an enterprise. We need a new generation of metrics that can enable enterprises to react even faster in order to properly protect mission-critical systems in the midst of both undiscovered and disclosed vulnerabilities. In this paper, we propose a practical and predictive security model for exploitability analysis in a networking environment using stochastic modeling. Our model is built upon the trusted CVSS Exploitability framework and we analyze how the atomic attributes namely Access Complexity, Access Vector and Authentication that make up the exploitability score evolve over a specific time period. We formally define a nonhomogeneous Markov model which incorporates time dependent covariates, namely the vulnerability age and the vulnerability discovery rate. The daily transition-probability matrices in our study are estimated using a combination of Frei's model & Alhazmi Malaiya's Logistic model. An exploitability analysis is conducted to show the feasibility and effectiveness of our proposed approach. Our approach enables enterprises to apply analytics using a predictive cyber security model to improve decision making and reduce risk.

S. Abraham and S. Nair, "A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015, pp. 774-781.

http://ieeexplore.ieee.org/document/7345354/

Evaluating the security of an enterprise is an important step towards securing its system and resources. However existing research provide limited insight into understanding the impact attacks have on the overall security goals of an enterprise. We still lack effective techniques to accurately measure the predictive security risk of an enterprise taking into account the dynamic attributes associated with vulnerabilities that can change over time. It is therefore critical to establish an effective cyber-security analytics strategy to minimize risk and protect critical infrastructure from external threats before it even starts. In this paper we present an integrated view of security for computer networks within an enterprise, understanding threats and vulnerabilities, performing analysis to evaluate the current as well as future security situation of an enterprise to address potential situations. We formally define a non-homogeneous Markov model for quantitative security

evaluation using Attack Graphs which incorporates time dependent covariates, namely the vulnerability age and the vulnerability discovery rate to help visualize the future security state of the network leading to actionable knowledge and insight. We present experimental results from applying this model on a sample network to demonstrate the practicality of our approach.

S. Abraham, S. Nair, "A Predictive Framework for Cyber Security Analysis Using Attack Graphs," International Journal of Computing Networks & Communications (IJCNC), vol. 7, no. 1, January 2015.

https://arxiv.org/abs/1502.01240

Security metrics serve as a powerful tool for organizations to understand the effectiveness of protecting computer networks. However majority of these measurement techniques don't adequately help corporations to make informed risk management decisions. In this paper we present a stochastic security framework for obtaining quantitative measures of security by taking into account the dynamic attributes associated with vulnerabilities that can change over time. Our model is novel as existing research in attack graph analysis do not consider the temporal aspects associated with the vulnerabilities, such as the availability of exploits and patches which can affect the overall network security based on how the vulnerabilities are interconnected and leveraged to compromise the system. In order to have a more realistic representation of how the security state of the network would vary over time, a nonhomogeneous model is developed which incorporates a time dependent covariate, namely the vulnerability age. The daily transition-probability matrices are estimated using Frei's Vulnerability Lifecycle model. We also leverage the trusted CVSS metric domain to analyze how the total exploitability and impact measures evolve over a time period for a given network.

A. Applebaum, D. Miller, B. Strom, C. Korban, R. Wolf, "Intelligent, automated red team emulation," *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pp. 363-373, 2016.

http://dl.acm.org/citation.cfm?id=2991111

Red teams play a critical part in assessing the security of a network by actively probing it for weakness and vulnerabilities. Unlike penetration testing - which is typically focused on exploiting vulnerabilities - red teams assess the entire state of a network by emulating real adversaries, including their techniques, tactics, procedures, and goals. Unfortunately, deploying red teams is prohibitive: cost, repeatability, and expertise all make it difficult to consistently employ red team tests. We seek to solve this problem by creating a framework for automated red team emulation, focused on what the red team does post-compromise - i.e., after the perimeter has been breached. Here, our program acts as an automated and intelligent red team, actively moving through the target network to test for weaknesses and train defenders. At its core, our framework uses an automated planner designed to accurately reason about future plans in the face of the vast amount of uncertainty in red teaming scenarios. Our solution is custom-developed, built on a logical encoding of the cyber environment and adversary profiles, using techniques from

classical planning, Markov decision processes, and Monte Carlo simulations. In this paper, we report on the development of our framework, focusing on our planning system. We have successfully validated our planner against other techniques via a custom simulation. Our tool itself has successfully been deployed to identify vulnerabilities and is currently used to train defending blue teams.

F. Cohen, "Simulating Cyber Attacks, Defences and Consequences," *Computers & Security*, vol. 18, no. 6, 1999, pages 479-518.

http://www.sciencedirect.com/science/article/pii/S0167404899801151

Many fields use modeling and simulation to provide analysis and insight into building better systems, but the field of information protection has not produced significant research results in this area to date. Perhaps this is due to the extreme complexity of the cyber attack and defense problem, the enormous size of the search space, the lack of good data on attacks and defenses, the inability to derive consequences in a systematic way, or the lack of a coherent view of information protection. Despite these sometimes seemingly unscalable barriers, this paper is about simulations of attacks, defenses, and consequences in complex cyber systems such as computer networks; and more specifically about one attempt to create simulations capable of providing meaningful results in this field.

We begin by discussing limitations on modeling and simulation that are relatively unique to information protection, discuss the model we chose, and how simulation works. Next we show results of individual simulations and runs of a few thousand simulations that characterize small portions of the design space for attacks alone and then attacks in the presence of defenses. We continue with issues of parallel simulation and demonstrate results from large-scale simulation runs involving scores of parallel processors covering millions of runs and varying several parameters of interest. Results are given for the effects of detection and reaction time on success rates, the effects of defender strength on success rate, non-linearities between strength and time and the effectiveness of a defense, and differences between results for varying threat profiles. We then add issues of costs and produce expected loss and cost results, discuss and demonstrate the effects of strategies on results, review limitations of metrics and sensitivity to variations in parameters, and briefly discuss validation of results.

K.C. Costantini, "Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis," Rochester Institute of Technology, October 2007.

http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=6703&context=theses

Computer networks are now relied on more than ever before for gathering information and performing essential business functions. In addition, cyber crime is frequently used as a means of exploiting these networks to obtain useful and private information. Although intrusion detection tools are available to assist in detecting malicious activity within a network, these tools often lack the ability to clearly identify cyber attacks. This limitation makes the development of effective tools an imperative task to assist in both detecting and taking action against cyber attacks as they occur. In developing such tools,

reliable test data must be provided that accurately represents the activities of networks and attackers without the large overhead of setting up physical networks and cyber attacks. The intent of this thesis is to use operation research and simulation techniques to provide both data and data-generation tools representative of real-world computer networks, cyber attacks, and security intrusion detection systems. A simulation model is developed to represent the structure of networks, the unique details of network devices, and the aspects of intrusion detection systems used within networks. The simulation is also capable of generating representative cyber attacks that accurately portray the capabilities of attackers and the intrusion detection alerts associated with the attacks. To ensure that the data provided is reliable, the simulation model is verified by evaluating the structure of the networks, cyber attacks, and sensor alerts, and validated by evaluating the accuracy of the data generated with respect to what occurs in a real network. By providing accurate data with respect to network structure, attack structure, and intrusion detection alerts, the simulation methods used offer considerable support in developing tools that can accurately detect and take action against attacks.

S. Creese, M. Goldsmith, N. Moffat, J. Happa and I. Agrafiotis, "CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise," *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2013, pp. 73-79.

http://ieeexplore.ieee.org/document/6698979/

A variety of data-mining tools and filtering techniques exist to detect and analyze cyber-attacks by monitoring network traffic. In recent years many of these tools use visualization designed to make traffic patterns and impact of an attack tangible to a security analyst. The visualizations attempt to facilitate understanding elements of an attack, including the location of malicious activity on a network and the consequences for the wider system. The human observer is able to detect patterns from useful visualizations, and so discover new knowledge about existing data sets. Because of human reasoning, such approaches still have an advantage over automated detection, data-mining and analysis. The core challenge still lies in using the appropriate visualization at the right time. It is this lack of situational awareness that our CyberVis framework is designed to address. In this paper we present a novel approach to the visualization of enterprise network attacks and their subsequent potential consequences. We achieve this by combining traditional network diagram icons with Business Process Modeling and Notation (BPMN), a risk-propagation logic that connects the network and business-process and task layer, and a flexible alert input schema able to support intrusion alerts from any third-party sensor. Rather than overwhelming a user with excessive amounts of information, CyberVis abstracts the visuals to show only noteworthy information about attack data and indicates potential impact both across the network and on enterprise tasks. CyberVis is designed with the Human Visual System (HVS) in mind, so severe attacks (or many smaller attacks that make up a large risk) appear more salient than other components in the scene. A Deep-Dive window allows for investigation of data, similar to a database interface. Finally, a Forensic Mode allows movie-style playback of past alerts under user-defined conditions for closer examination.

Duggan, D.P., Thomas, S.R., Veitch, C.K.K., and Woodard, L., "Categorizing Threat: Building and Using a Generic Threat Matrix," SAND2007-5791, 2007, Sandia National Laboratories.

The key piece of knowledge necessary for building defenses capable of withstanding or surviving cyber and kinetic attacks is an understanding of the capabilities posed by threats to a government, function, or system. With the number of threats continuing to increase, it is no longer feasible to enumerate the capabilities of all known threats and then build defenses based on those threats that are considered, at the time, to be the most relevant. Exacerbating the problem for critical infrastructure entities is the fact that the majority of detailed threat information for higher-level threats is held in classified status and is not available for general use, such as the design of defenses and the development of mitigation strategies. To reduce the complexity of analyzing threat, the threat space must first be reduced. This is achieved by taking the continuous nature of the threat space and creating an abstraction that allows the entire space to be grouped, based on measurable attributes, into a small number of distinctly different levels. The work documented in this report is an effort to create such an abstraction.

P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, February–March 2009.

http://www.sciencedirect.com/science/article/pii/S0167404808000692

The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. In this context, anomaly-based network intrusion detection techniques are a valuable technology to protect target systems and networks against malicious activities. However, despite the variety of such methods described in the literature in recent years, security tools incorporating anomaly detection functionalities are just starting to appear, and several important problems remain to be solved. This paper begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues.

H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, "P^{2}CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 626-639, Nov.-Dec. 1 2015.

http://ieeexplore.ieee.org/document/6990572/

This paper presents the Predictive, Probabilistic Cyber Security Modeling Language (P^{2}CySeMoL), an attack graph tool that can be used to estimate the cyber security of enterprise architectures. P^{2}CySeMoL includes theory on how attacks and defenses relate quantitatively; thus, users must only model their assets and how these are connected in order to enable calculations. The performance of P^{2}CySeMoL enables quick calculations

of large object models. It has been validated on both a component level and a system level using literature, domain experts, surveys, observations, experiments and case studies.

J. B. Hong, D. S. Kim and A. Haqiq, "What Vulnerability Do We Need to Patch First?," *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Atlanta, GA, 2014, pp. 684-689.

http://ieeexplore.ieee.org/document/6903625/

Computing a prioritized set of vulnerabilities to patch is important for system administrators to determine the order of vulnerabilities to be patched that are more critical to the network security. One way to assess and analyze security to find vulnerabilities to be patched is to use attack representation models (ARMs). However, security solutions using ARMs are optimized for only the current state of the networked system. Therefore, the ARM must reanalyze the network security, causing multiple iterations of the same task to obtain the prioritized set of vulnerabilities to patch. To address this problem, we propose to use importance measures to rank network hosts and vulnerabilities, then combine these measures to prioritize the order of vulnerabilities to be patched. We show that nearly equivalent prioritized set of vulnerabilities can be computed in comparison to an exhaustive search method in various network scenarios, while the performance of computing the set is dramatically improved, while equivalent solutions are computed in various network scenarios.

I. Kotenko and A. Chechulin, "A Cyber Attack Modeling and Impact Assessment framework," *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, 2013, pp. 1-24.

http://ieeexplore.ieee.org/document/6568374/

The paper suggests a framework for cyber attack modeling and impact assessment. It is supposed that the common approach to attack modeling and impact assessment is based on representing malefactors' behavior, generating attack graphs, calculating security metrics and providing risk analysis procedures. The main aspects outlined are achieving near-real time mode, event analysis and prognosis mechanisms, security and impact assessment. To optimize the attack graph generation and security evaluation we apply an anytime approach to have the result at any time by applying a set of algorithms with different timelines and precision. The architecture of the Cyber Attack Modeling and Impact Assessment Component (CAMIAC) is proposed. We present the prototype of the component, the results of experiments carried out, and comparative analysis of the techniques used.

M. E. Kuhl, M. Sudit, J. Kistner and K. Costantini, "Cyber attack modeling and simulation for network security analysis," *2007 Winter Simulation Conference*, Washington, DC, 2007, pp. 1180-1188.

http://ieeexplore.ieee.org/document/4419720/

Cyber security methods are continually being developed. To test these methods many organizations utilize both virtual and physical networks which can be costly and time consuming. As an alternative, in this paper, we present a simulation modeling approach to represent computer networks and intrusion detection systems (IDS) to efficiently simulate cyber attack scenarios. The outcome of the simulation model is a set of IDS alerts that can be used to test and evaluate cyber security systems. In particular, the simulation methodology is designed to test information fusion systems for cyber security that are under development.

Jang-Se Lee, Jung-Rae Jung, Jong-Sou Park, Sung-Do Chi, "Linux-Based System Modelling for Cyber-attack Simulation," In: Kim T.G. (eds) Artificial Intelligence and Simulation. AIS 2004. Lecture Notes in Computer Science, vol 3397, Springer, Berlin, Heidelberg.

https://link.springer.com/chapter/10.1007%2F978-3-540-30583-5_62

The major objective of this paper is to describe modeling on the linux-based system for simulation of cyber attacks. To do this, we have analyzed the Linux system from a security viewpoint and proposed the Linux-based system model using the DEVS modeling and simulation environment. Unlike conventional researches, we are able to i) reproduce the detail behavior of cyber-attack, ii) analyze concrete changes of system resource according to a cyber-attack and iii) expect that this would be a cornerstone for more practical application researches (generating cyber-attack scenarios, analyzing urban vulnerability and examining countermeasures, etc.) of security simulation. Several simulation tests performed on sample network system will illustrate our techniques.

Lee-Urban S., Whitaker E., Riley M., Trewhitt E. (2016) Two Complementary Network Modeling and Simulation Approaches to Aid in Understanding Advanced Cyber Threats. In: Nicholson D. (eds) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol 501. Springer, Cham

https://link.springer.com/chapter/10.1007/978-3-319-41932-9_33

This paper describes two complementary approaches to modeling and simulation (M&S) of sophisticated malware attacks for their use in understanding and preparing for potential threats. Modern malware operates at multiple scales, and successfully defending against these attacks requires the ability to understand the effects of decisions across this range. We present two types of M&S frameworks that differ in fidelity and scalability. The first is a low fidelity, scalable approach for representing and studying the spread of malware in a large network at a macro scale. The network is both modelled and simulated in ns-3, a discrete event simulation tool typically used for protocol exploration and traffic monitoring that supports the simulation of tens of thousands of nodes. The second type of simulation is a higher-fidelity, micro scale approach that includes nodes that closely emulate the behavior of actual computer systems and may include real hardware and software. Ns-3 allows outside networks to interact in real-time with ns-3. This enables the combination of the network simulation environment with real and virtual machines to allow detailed observation of the ways in which a hypothetical advanced persistent threat would play out in a small subnetwork. The interface between the ns-3 simulation, attack

framework (e.g. Metasploit), and the real and virtual nodes is managed by a controller that also supplies configuration, business logic and results logging. We present use cases for both simulation types, showing how each approach can be used in the analysis of malware.

R. P. Lippmann, K. W. Ingols, C. Scott, K. Piwowarski, K. J. Kratkiewicz, M. Artz, and R. K. Cunningham, "Evaluating and Strengthening Enterprise Network Security Using Attach Graphs," ESC-TR-2005-064, Lincoln Laboratory.

https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/0507_Lippmann.pdf

Assessing the security of large enterprise networks is complex and labor intensive. Current security analysis tools typically examine only individual firewalls, routers, or hosts separately and do not comprehensively analyze overall network security. We present a new approach that uses configuration information on firewalls and vulnerability information on all network devices to build attack graphs that show how far inside and outside attackers can progress through a network by successively compromising exposed and vulnerable hosts. In addition, attack graphs are automatically analyzed to produce a small set of prioritized recommendations to enhance network security. Field trials on networks with up to 3,400 hosts demonstrate the ability to accurately identify a small number of critical stepping-stone hosts that need to be patched to protect against external attackers. Simulation studies on complex networks with more than 40,000 hosts demonstrate good scaling. This analysis can be used for many purposes, including identifying critical stepping-stone hosts to patch or protect with a firewall, comparing the security of alternative network designs, determining the security risk caused by proposed changes in firewall rules or new vulnerabilities, and identifying the most critical hosts to patch when a new vulnerability is announced. Unique aspects of this work are new attack graph generation algorithms that scale to enterprise networks with thousands of hosts, efficient approaches to determine what other hosts and ports in large networks are reachable from each individual host, automatic data importation from network vulnerability scanners and firewalls, and automatic attack graph analyses to generate recommendations.

P. Maggi, D. Pozza and R. Sisto, "Vulnerability Modelling for the Analysis of Network Attacks," *2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX*, Szklarska Poreba, 2008, pp. 15-22.

http://ieeexplore.ieee.org/document/4573035/

In order to perform a successful attack on a network, an intruder must know various penetration techniques, also known as exploits. In general, an exploit can be successful only if some pre-conditions are true. Such conditions may involve the presence of vulnerable programs and/or specific software configurations, as well as certain attacker privileges on hosts and network reachability. When an exploit has success, it usually induces a new set of conditions within the network (post-conditions), such as new attacker privileges, and increased connectivity. Therefore, a network attack can be made

of a series of exploits that gradually increase the attacker "power" on the network, until some final goal has been reached or the whole network has been compromised. Reaching such a goal is possible because of dependencies among exploits in terms of pre- and post-conditions. This paper describes how the OVAL language, originally aimed at describing how to check for the existence of vulnerabilities on hosts, can be enhanced to allow automatic reasoning for precisely determining the possible chains of exploits that an attacker could use to compromise the hosts in the network. Moreover, the paper shows how the description of vulnerabilities can be enriched to allow performing risk analysis, so as to determine the impact of attackers on the network, as well as the likelihood of attacks.

D. M. Nicol, J. Liu, M. Liljenstam and Guanhua Yan, "Simulation of large scale networks using SSF," *Proceedings of the 2003 Winter Simulation Conference, 2003.*, 2003, pp. 650-657 Vol.1.

http://ieeexplore.ieee.org/document/1261480/

Some applications of simulation require that the model state be advanced in simulation time faster than the wall-clock time advances as the simulation executes. This "faster than real-time" requirement is crucial, for instance, when a simulation is used as part of a real-time control system, working through the consequences of contemplated control actions, in order to identify feasible (or even optimal) decisions. This paper considers the issue of faster than real-time simulation of very large communication networks, and how this is accomplished using our implementation (in C++) of the scalable simulation framework (SSF). Our tool (called iSSF) uses hierarchical levels of abstraction, and parallelism, to achieve speedups of nearly four orders of magnitude, enabling real-time execution rates on large network models. We quantify the effects that choice of hierarchical abstraction has on the simulation time advance rate, and show analytically and empirically how changing the abstraction mix affects performance.

M. A. Rahman and E. Al-Shaer, "A formal approach for network security management based on qualitative risk analysis," *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, Ghent, 2013, pp. 244-251.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6572992&isnumber=6572961

The risk analysis is an important process for enforcing and strengthening efficient and effective security. Due to the significant growth of the Internet, application services, and associated security attacks, information professionals face challenges in assessing risk of their networks. The assessment of risk may vary with the enterprise's requirements. Hence, a generic risk analysis technique is suitable. Moreover, configuring a network with correct security policy is a difficult problem. The assessment of risk aids in realizing necessary security policy. Risk is a function of security threat and impact. Security threats depend on the traffic reachability. Security devices like firewalls are used to selectively allow or deny traffic. However, the connection between the network risk and the security policy is not easy to establish. A small modification in the network topology or in the security policy, can change the risk significantly. It is hard to manually follow a systematic process for configuring the network towards security hardening. Hence, an

automatic generation of proper security controls, e.g., firewall rules and host placements in the network topology, is crucial to keep the overall security risk low. In this paper, we first present a declarative model for the qualitative risk analysis. We consider transitive reachability, i.e., reachability considering one or more intermediate hosts, in order to compute exposure of vulnerabilities. Next, we formalize our risk analysis model and the security requirements as a constraint satisfaction problem using the satisfiability modulo theories (SMT). A solution to the problem synthesizes necessary firewall policies and host placements. We also evaluate the scalability of the proposed risk analysis technique as well as the synthesis model.

G. Rasche, E. Allwein, M. Moore and B. Abbott, "Model-Based Cyber Security," *14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07)*, Tucson, AZ, 2007, pp. 405-412.

http://ieeexplore.ieee.org/document/4148957/

This paper presents an approach for automatically verifying the correctness of cyber security applications through formal analysis guided by hierarchical models of the network, its applications, and potential attacks. This work is motivated by the need for a more intuitive, automated systems-level approach to determining the overall security characteristics of a large network. Given the complex nature of security tools and their general lack of interoperability, it is difficult for system designers to make definitive statements about the nature of their network defense. Our work focuses on creating an environment in which security experts can model the security aspects of complex networks using a graphical notation that is intuitive and natural for them, then automatically perform security activities such as formally verifying the safety of the network against known threats and exploring the network design for potential vulnerabilities. The environment is designed to utilize third party tools for performing these activities and concentrates on integration of these tools within a common modeling framework.

N. Soule *et al*., "Quantifying & minimizing attack surfaces containing moving target defenses," *2015 Resilience Week (RWS)*, Philadelphia, PA, 2015, pp. 1-6.

http://ieeexplore.ieee.org/document/7287449/

The cyber security exposure of resilient systems is frequently described as an attack surface. A larger surface area indicates increased exposure to threats and a higher risk of compromise. Ad-hoc addition of dynamic proactive defenses to distributed systems may inadvertently increase the attack surface. This can lead to cyber friendly fire, a condition in which adding superfluous or incorrectly configured cyber defenses unintentionally reduces security and harms mission effectiveness. Examples of cyber friendly fire include defenses which themselves expose vulnerabilities (e.g., through an unsecured admin tool), unknown interaction effects between existing and new defenses causing brittleness or unavailability, and new defenses which may provide security benefits, but cause a significant performance impact leading to mission failure through timeliness violations. This paper describes a prototype service capability for creating semantic models of attack

surfaces and using those models to (1) automatically quantify and compare cost and security metrics across multiple surfaces, covering both system and defense aspects, and (2) automatically identify opportunities for minimizing attack surfaces, e.g., by removing interactions that are not required for successful mission execution.

M. Välja, M. Korman, K. Shahzad and P. Johnson, "Integrated Metamodel for Security Analysis," *2015 48th Hawaii International Conference on System Sciences*, Kauai, HI, 2015, pp. 5192-5200.

http://ieeexplore.ieee.org/document/7070437/

This paper proposes a metamodel for analyzing security aspects of enterprise architecture by combining analysis of cybersecurity with analysis of interoperability and availability. The metamodel extends an existing attack graph based metamodel for cyber security modeling and evaluation, P^{2}CySeMoL, and incorporates several new elements and evaluation rules. The approach improves security analysis by combining two ways of evaluating reach ability: one which considers ordinary user activity and another, which considers technically advanced techniques for penetration and attack. It is thus permitting to evaluate security in interoperability terms by revealing attack possibilities of legitimate users. Combined with data import from various sources, like an enterprise architecture data repository, the instantiations of the proposed metamodel allow for a more holistic overview of the threats to the architecture than the previous version. Additional granularity is added to the analysis with the reach ability need concept and by enabling the consideration of unavailable and unreliable systems.

Y. Wang, C. Lin and K. Meng, "Security Analysis of Enterprise Network Based on Stochastic Game Nets Model," *2009 IEEE International Conference on Communications*, Dresden, 2009, pp. 1-5.

http://ieeexplore.ieee.org/document/5199442/

In this paper, we propose a novel modeling method, Stochastic Game Nets (SGN), and use it to model and analyze the security issues in enterprise networks. Firstly, the definition and modeling algorithm of Stochastic Game Nets are given. And then we apply the Stochastic Game Nets method to describe the attack and defense course in the enterprise networks successfully, and find a Nash equilibrium. Finally we analyze the confidentiality and integrity of the enterprise network quantificationally [sic] based on the model. The method can also be applied to other areas with respect to a game.

Peng Xie, J. H. Li, Xinming Ou, Peng Liu and R. Levy, "Using Bayesian networks for cyber security analysis," *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, Chicago, IL, 2010, pp. 211-220.

http://ieeexplore.ieee.org/document/5544924/

Capturing the uncertain aspects in cyber security is important for security analysis in enterprise networks. However, there has been insufficient effort in studying what modeling approaches correctly capture such uncertainty, and how to construct the models

to make them useful in practice. In this paper, we present our work on justifying uncertainty modeling for cyber security, and initial evidence indicating that it is a useful approach. Our work is centered around near real-time security analysis such as intrusion response. We need to know what is really happening, the scope and severity level, possible consequences, and potential countermeasures. We report our current efforts on identifying the important types of uncertainty and on using Bayesian networks to capture them for enhanced security analysis. We build an example Bayesian network based on a current security graph model, justify our modeling approach through attack semantics and experimental study, and show that the resulting Bayesian network is not sensitive to parameter perturbation.

S. E. Yusuf, M. Ge, J. B. Hong, H. K. Kim, P. Kim and D. S. Kim, "Security Modelling and Analysis of Dynamic Enterprise Networks," *2016 IEEE International Conference on Computer and Information Technology (CIT)*, Nadi, 2016, pp. 249-256.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7876345

Dynamic networks can be characterized by many factors such as changes (e.g., vulnerability change, update of applications and services, topology changes). It is of vital importance to assess the security of such dynamic networks in order to improve the security of them. One way to assess the security is to use a graphical security model. However, the existing graphical security models (e.g., attack graphs and attack trees) have only considered static networks (i.e. the network does not change). It is also unclear how the existing cyber security metrics (e.g., attack cost, shortest attack path) change when the network configuration changes over time. To address this problem, we propose (i) to develop a novel graphical security model named Temporal-Hierarchical Attack Representation Model (T-HARM) to capture network changes and (ii) investigate the effect of network change on the existing cyber security metrics based on the proposed security model. We show how the existing security metrics change when the status of vulnerabilities changes.

Cyber-Physical Systems

C. Cheh, G. A. Weaver and W. H. Sanders, "Cyber-Physical Topology Language: Definition, Operations, and Application," *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*, Zhangjiajie, 2015, pp. 60-69.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7371849&isnumber=7371833

Maintaining the resilience of a large-scale system requires an accurate view of the system's cyber and physical state. The ability to collect, organize, and analyze state central to a system's operation is thus important in today's environment, in which the number and sophistication of security attacks are increasing. Although a variety of "sensors" (e.g., Intrusion Detection Systems, log files, and physical sensors) are available to collect system state information, it's difficult for administrators to maintain and analyze the diversity of information needed to understand a system's security state. Therefore, we have developed the Cyber-Physical Topology Language (CPTL) to

represent and reason about system security. CPTL combines ideas from graph theory and formal logics, and provides a framework to capture relationships among the diverse types of sensor information. In this paper, we formally define CPTL as well as operations on CPTL models that can be used to infer a system's security state. We then illustrate the use of CPTL in both the enterprise and electrical power domains and provide experimental results that illustrate the practicality of the approach.

P. Y. Chen, S. M. Cheng and K. C. Chen, "Smart attacks in smart grid communication networks," in *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24-29, August 2012.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6257523&isnumber=6257514

The operations of a smart grid heavily rely on the support of communication infrastructures for efficient electricity management and reliable power distribution. Due to the strong dependency, the robustness of a smart grid communication network against attack is of the utmost importance for the deployment of the smart grid. Notably, the large scale and autonomous features of a smart grid render its cyber security quite vulnerable to adversaries. In this article, we introduce several intelligent attacks and countermeasures in smart grid communication networks, which aim for maximal damage or benefits by taking advantage of the network structure as well as the protocol functionality. We adopt the percolation-based connectivity in statistic mechanics to quantitatively analyze the network robustness. If the attack and defense strategies are involved, the attack can be further smart and complicated. Consequently, a two player zero-sum game is introduced between the adversary and the defender, and the outcome of the game equilibrium is used to evaluate the performance of defense mechanisms with different network configurations. This article therefore offers novel insights and comprehensive analysis on the cyber security of a smart grid.

K. R. Davis *et al*., "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464-2475, Sept. 2015.

http://ieeexplore.ieee.org/document/7103368/

The integration of cyber communications and control systems into the power grid infrastructure is widespread and has a profound impact on the operation, reliability, and efficiency of the grid. Cyber technologies allow for efficient management of the power system, but they may contain vulnerabilities that need to be managed. One important possible consequence is the introduction of cyber-induced or cyber-enabled disruptions of physical components. In this paper, we propose an online framework for assessing the operational reliability impacts due to threats to the cyber infrastructure. This framework is an important step toward addressing the critical challenge of understanding and analyzing complex cyber-physical systems at scale.

Z. Drias, A. Serhrouchni and O. Vogel, "Analysis of cyber security for industrial control systems," *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, 2015, pp. 1-8.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7245330&isnumber=7245317

Industrial control systems (ICS) are specialized information systems that differs significantly form traditional information systems used in the IT world. The main use of ICS is to manage critical infrastructures such as, Oil and Natural Gas facilities, nuclear plants, smart grids, water and waste water…etc. ICS have many unique functional characteristics, including a need for real-time response and extremely high availability, predictability, reliability, as well as distributed intelligence. Which for, many advanced computing, communication and internet technologies were integrated to the ICS to cover more costumers requirements such as mobility, data analytics, extensibility…etc The integration of these technologies makes from the ICS open systems to the external world; this openness exposes the critical infrastructures to several Cyber security critical issues. Nowadays, cyber security emerges to be one of the most critical issues because of the immediate impact and the high cost of cyber-attacks. In this paper, we present a comprehensive analysis of cyber security issues for ICS. Specifically we focus on discussing and reviewing the different types and architectures of an ICS, security requirements, different threats attacks, and existing solutions to secure Industrial control systems. By this survey, we desire to provide a clear understanding of security issues in ICS and clarify the different research issues to solve in the future.

A. Easwaran, A. Chattopadhyay and S. Bhasin, "A systematic security analysis of real-time cyber-physical systems," *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, Chiba, 2017, pp. 206-213.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7858321&isnumber=7858249

Security in Cyber-Physical Systems (CPS) has become a serious concern owing to the rapid adoption of technologies such as plug-and-play connectivity, robotics and remote coordination and control. It is well understood that the performance overhead incurred due to security considerations is rather high which needs to be captured holistically for a real-time CPS with strict timing budget and hard deadlines. Additionally, attacks in real-time CPS may only alter the timing behavior of system components without any changes in functionality, resulting in serious consequences due to missed deadlines. To address this challenging issue, it is necessary to understand the role of diverse components in a real-time CPS and how those expose the system to a malicious attacker. In this paper, we propose a systematic security analysis flow, using a novel Attack Sequence Diagram (ASD), which links the sources, intermediate components and final manifestations of an attack, thereby clearly delineating the attack surfaces of a complex real-time CPS. Based on the ASD, it is possible to evaluate the complexity of an attack, performance overhead of a countermeasure and explore different design trade-offs for a real time CPS. With the help of real-world and synthetic examples, we demonstrate that ASD seamlessly enables one to map the existing vulnerabilities and uncover new attack possibilities.

M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, 2009, pp. 1-6.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4840267&isnumber=4839920

Enterprise architecture is a rising discipline that is gaining increasing interest in both industry and academia. It pays attention to the fact that effective management of business and IT needs take a holistic view of the enterprise. Enterprise architecture is based on graphical models as a vehicle for system analysis, design, and communication. Enterprise architecture is also a potential support for control systems management. Unfortunately, when it comes to security analyses, the architectural languages available are not adapted to provide support for this. This presentation focus on research performed as part of the EU seventh framework program VIKING (Vital Infrastructure, Networks, Information and Control Systems Management) and the Swedish Centre of Excellence in Electric Power Engineering, EKC2. The research is focusing on developing and adapting security analyses frameworks to architectural languages on a level where information about control systems' configuration is scarce and thus incomplete and partly unreliable.

S. Jauhar *et al.*, "Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios," *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*, Zhangjiajie, 2015, pp. 319-324.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7371879&isnumber=7371833

The transformation of traditional power systems to smart grids brings significant benefits, but also exposes the grids to various cyber threats. The recent effort led by US National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 to compile failure scenarios is an important initiative to document typical cybersecurity threats to smart grids. While these scenarios are an invaluable thought-aid, companies still face challenges in systematically and efficiently applying the failure scenarios to assess security risks for their specific infrastructure. In this work, we develop a model-based process for assessing the security risks from NESCOR failure scenarios. We extend our cybersecurity assessment tool, Cyber- SAGE, to support this process, and use it to analyze 25 failure scenarios. Our results show that CyberSAGE can generate precise and structured security argument graphs to quantitatively reason about the risk of each failure scenario. Further, CyberSAGE can significantly reduce the assessment effort by allowing the reuse of models across different failure scenarios, systems, and attacker profiles to perform "what if?" analysis.

R. Kalluri, L. Mahendra, R. K. S. Kumar and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," *2016 National Power Systems Conference (NPSC)*, Bhubaneswar, 2016, pp. 1-5.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7858908&isnumber=7858833

With ever growing threat of cyber terrorism, vulnerability of the Supervisory Control and Data Acquisition (SCADA) systems is the most common subject for most security researchers now. Attacks on SCADA systems are increasing and its impact needs to be studied to implement proper counter measures. Many of the SCADA systems are relatively insecure with chronic and pervasive vulnerabilities. This paper explains possible vulnerabilities present in SCADA systems and also present the impact analysis of Denial of Service (DoS) by modeling attack using influence diagram. Simulation of

DoS attacks will help in analyzing and accessing the security of SCADA system and also used to analyze the impact. Experiments have been conducted on RTU by targeting "availability" of the system, results have been analyzed and impact has been studied.

T. Kiesling, M. Krempel, J. Niederl and J. Ziegler, "A Model-Based Approach for Aviation Cyber Security Risk Assessment," *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, 2016, pp. 517-525.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7784614&isnumber=7784494

The air transport infrastructure is an attractive target for cyber attacks due to its importance and prominence. The current system is already vulnerable and the advent of more automation and pervasion of standard IT in the future leads to ever more complex and interconnected systems with an increasing attack surface. To cope with this situation, we need suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations. We propose a model-based approach for aviation cyber security risk assessment in support of holistic understanding of threats and risk in complex interconnected systems. We introduce our modeling approach and show how computer-based reasoning can be used for threat and risk analysis based on these models. This paper presents the promising results of initial research. Substantial effort is still needed to mature the approach. We expect major challenges to be of an organizational rather than technical nature.

X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," in *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 572-580, March 2017.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7439817&isnumber=7857818

This paper presents a risk assessment method for evaluating the cyber security of power systems considering the role of protection systems. This paper considers the impact of bus and transmission line protection systems located in substations on the cyber-physical performance of power systems. The proposed method simulates the physical response of power systems to malicious attacks on protection system settings and parameters. The relationship among settings of protection devices, protection logics, and circuit breaker logics is analyzed. The expected load curtailment (ELC) index is used in this paper to quantify potential system losses due to cyber attacks. The Monte Carlo simulation is applied to calculate ELC for assessing attackers' capabilities as bus arrangements are altered. The effectiveness of the proposed risk assessment method is demonstrated using a 9-bus system and the IEEE 68-bus system.

Ma Z., Smith P. (2013) Determining Risks from Advanced Multi-step Attacks to Critical Information Infrastructures. In: Luiijf E., Hartel P. (eds) Critical Information Infrastructures Security. CRITIS 2013. Lecture Notes in Computer Science, vol 8328. Springer, Cham

https://link.springer.com/chapter/10.1007/978-3-319-03964-0_13

Industrial Control Systems (ICS) monitor and control industrial processes, and enable automation in industry facilities. Many of these facilities are regarded as Critical Infrastructures (CIs). Due to the increasing use of Commercial-Off-The-Shelf (COTS) IT products and connectivity offerings, CIs have become an attractive target for cyber-attacks. A successful attack could have significant consequences. An important step in securing Critical Information Infrastructures (CIIs) against cyber-attacks is risk analysis – understanding security risks, based on a systematic analysis of information on vulnerabilities, cyber threats, and the impacts related to the targeted system. Existing risk analysis approaches have various limitations, such as scalability and practicability problems. In contrast to previous work, we propose a practical and *vulnerability-centric* risk analysis approach for determining security risks associated with advanced, multi-step cyber-attacks. In order to examine multi-step attacks that exploit chains of vulnerabilities, we map vulnerabilities into *preconditions* and *effects*, and use *rule-based reasoning* for identifying advanced attacks and their path through a CII.

M. Masera, I. Nai Fovino, 2006, Modelling Information Assets for Security Risk Assessment in Industrial Settings, The 15th EICAR Annual Conference Proceeding, pp. 137-149.

https://www.researchgate.net/publication/228953438_Modelling_information_assets_for_security_risk_assessment_in_industrial_settings

Industry has begun in the last years to take into consideration the use of Public Information Infrastructures (including the Internet) for remotely monitoring, managing and maintaining their technical systems. Concurrently, technical and business information systems are getting interconnected both through private and public networks. As a result, industry is exposed to internal and external cyber-threats, and the security assessment of the ICT infrastructures assumes a predominant relevance. However, underlying every useful security methodology there is a system description which decomposes the system in term of services, component, relationships and assets. In this paper, we focus our attention on a particular type of system asset to which, to our knowledge, the usual security assessment methodologies do not pay sufficient attention, the information asset. Such an asset, in fact, represents the core of every ICT infrastructure (commands sent to components are information assets, data stored into databases are information assets, data flowing through the network are information assets); therefore we believe that its proper description and analysis is key for assuring reliable results for security assessments. Starting from some classical definitions of information and knowledge, we examine this type of asset aiming at identifying the more suitable representation with respect to its security attributes. In more detail, we identify as interesting properties the interdependence between information assets, their life cycles, their dynamics (i.e. the flows of the information assets within the system), their topological location (in term of subsystems that hosts the information assets) and the correlation between the information assets and the vulnerabilities affecting the components of the system. We provide then a formal modelling framework for describing the characteristics of the information assets under a security assessment perspective.

M.J. McDonald, J. Mulder, B.T. Richardson, R.H. Cassidy, A. Chavez, N.D. Pattengale, G.M. Pollock, J.M. Urrea, M.D. Schwartz, W.D. Atkins, R.D. Halbgewachs, “Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications,” SAND2010-0568, 2010, Sandia National Laboratories, Albuquerque, New Mexico.

http://prod.sandia.gov/techlib/access-control.cgi/2010/100568.pdf

This paper describes a new hybrid modeling and simulation architecture developed at Sandia for understanding and developing protections against and mitigations for cyber threats upon control systems. It first outlines the challenges to PCS security that can be addressed using these technologies. The paper then describes Virtual Control System Environments (VCSE) that use this approach and briefly discusses security research that Sandia has performed using VCSE. It closes with recommendations to the control systems security community for applying this valuable technology.

Y. Mo *et al*., "Cyber–Physical Security of a Smart Grid Infrastructure," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

http://ieeexplore.ieee.org/document/6016202/

It is often appealing to assume that existing solutions can be directly applied to emerging engineering domains. Unfortunately, careful investigation of the unique challenges presented by new domains exposes its idiosyncrasies, thus often requiring new approaches and solutions. In this paper, we argue that the smart grid, replacing its incredibly successful and reliable predecessor, poses a series of new security challenges, among others, that require novel approaches to the field of cyber security. We will call this new field cyber– physical security. The tight coupling between information and communication technologies and physical systems introduces new security concerns, requiring a rethinking of the commonly used objectives and methods. Existing security approaches are either inapplicable, not viable, insufficiently scalable, incompatible, or simply inadequate to address the challenges posed by highly complex environments such as the smart grid. A concerted effort by the entire industry, the research community, and the policy makers is required to achieve the vision of a secure smart grid infrastructure.

Phu H. Nguyen, Shaukat Ali, Tao Yue, “Model-based security engineering for cyber-physical systems: A systematic mapping study,” in *Information and Software Technology*, vol. 83, March 2017, pp. 116-135.

http://www.sciencedirect.com/science/article/pii/S0950584916303214

Cyber-physical systems (CPSs) have emerged to be the next generation of engineered systems driving the so-called fourth industrial revolution. CPSs are becoming more complex, open and more prone to security threats, which urges security to be engineered systematically into CPSs. Model-Based Security Engineering (MBSE) could be a key means to tackle this challenge via security by design, abstraction, and automation. *Objective:* We aim at providing an initial assessment of the state of the art in MBSE for CPSs (MBSE4CPS). Specifically, this work focuses on finding out 1) the publication statistics of MBSE4CPS studies; 2) the characteristics of MBSE4CPS studies; and 3) the

open issues of MBSE4CPS research. *Method:* We conducted a systematic mapping study (SMS) following a rigorous protocol that was developed based on the state-of-the-art SMS and systematic review guidelines. From thousands of relevant publications, we systematically identified 48 primary MBSE4CPS studies for data extraction and synthesis to answer predefined research questions. *Results:* SMS results show that for three recent years (2014–2016) the number of primary MBSE4CPS studies has increased significantly. Within the primary studies, the popularity of using Domain-Specific Languages (DSLs) is comparable with the use of the standardized UML modelling notation. Most primary studies do not explicitly address specific security concerns (e.g., confidentiality, integrity) but rather focus on security analyses in general on threats, attacks or vulnerabilities. Few primary studies propose to engineer security solutions for CPSs. Many focus on the early stages of development lifecycle such as security requirement engineering or analysis. *Conclusion:* The SMS does not only provide the state of the art in MBSE4CPS, but also points out several open issues that would deserve more investigation, e.g., the lack of engineering security solutions for CPSs, limited tool support, too few industrial case studies, and the challenge of bridging DSLs in engineering secure CPSs.

H. Orojloo and M. A. Azgomi, "A method for modeling and evaluation of the security of cyber-physical systems," *2014 11th International ISC Conference on Information Security and Cryptology*, Tehran, 2014, pp. 131-136.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6994036&isnumber=6994006

Quantitative evaluation of security has always been one of the challenges in the field of computer security. The integration of computing and communication technologies with physical components, has introduced a variety of new security risks, which threaten cyber-physical components. It is possible that an attacker damage a physical component with cyber attack. In this paper, we propose a new approach for modeling and quantitative evaluation of the security of cyber-physical systems (CPS). The proposed method, considers those cyber attacks that can lead to physical damages. The factors impacting attacker's decision-making in the process of cyber attack to cyber-physical system are also taken into account. Furthermore, for describing the attacker and the system behaviors over time, the uniform probability distributions are used in a state-based semi-Markov chain (SMC) model. The security analysis is carried out for mean time to security failure (MTTSF), steady-state security, and steady-state physical availability.

F. Pasqualetti, F. Dörfler and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," *2011 50th IEEE Conference on Decision and Control and European Control Conference*, Orlando, FL, USA, 2011, pp. 2195-2201.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6160641&isnumber=6159299

Future power networks will be characterized by safe and reliable functionality against physical and cyber attacks. This paper proposes a unified framework and advanced monitoring procedures to detect and identify network components malfunction or

measurements corruption caused by an omniscient adversary. We model a power system under cyber physical attack as a linear time-invariant descriptor system with unknown inputs. Our attack model generalizes the prototypical stealth, (dynamic) false-data injection and replay attacks. We characterize the fundamental limitations of both static and dynamic procedures for attack detection and identification. Additionally, we design provably-correct (dynamic) detection and identification procedures based on tools from geometric control theory. Finally, we illustrate the effectiveness of our method through a comparison with existing (static) detection algorithms, and through a numerical study.

P. Palensky, E. Widl and A. Elsheikh, "Simulating Cyber-Physical Energy Systems: Challenges, Tools and Methods," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 3, pp. 318-326, March 2014.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6623196&isnumber=6739146

The energy system of the future is expected to be composed of a large variety of technologies and applications. However, the diverse nature of these components, their interlinked topology, and the sheer size of the system lead to an unprecedented level of complexity. Industry is confronted with severe problems in designing interoperable grid components, analyzing system stability, and improving efficiency. This paper describes the main challenges of continuous time-based and discrete event-based models of such cyber-physical energy systems. Using a characteristic test model, the scalability of the two approaches is analyzed. The results show the strengths and weaknesses of these two fundamentally different modeling principles that need to be considered when working with large scale cyber-physical energy systems.

A. Rodríguez-Mota, P. J. Escamilla-Ambrosio, J. Happa and J. R. C. Nurse, "Towards IoT cybersecurity modeling: From malware analysis data to IoT system representation," *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, Medellin, 2016, pp. 1-6.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7811597&isnumber=7811551

The heterogeneous nature of the Internet of Things (IoT) represents a big challenge in many different technical and scientific areas, among them Security. In this sense, security becomes an extremely complex problem as it is present in every aspect of the IoT ecosystem, from sensors and data acquisition hardware to front-end software applications and sophisticated user devices. This complexity expands as there is not consensus among all stakeholders towards the definition of general technical standards, specifications, system representations and use policies. In this context, this paper presents a state of intention for a research project oriented to construct a set of tools to characterize security attack surfaces for IoT systems solutions. The proposed research includes the development of a visual grammar aimed to depict IoT systems at a high-abstraction level together with the construction of objects profiles, which in conjunction will provide building blocks and mechanisms to evaluate or identify insecure IoT scenarios.

K. C. Sou, H. Sandberg and K. H. Johansson, "On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem," in *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 856-865, June 2013.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6473867&isnumber=6517533

This paper considers a smart grid cyber-security problem analyzing the vulnerabilities of electric power networks to false data attacks. The analysis problem is related to a constrained cardinality minimization problem. The main result shows that an relaxation technique provides an exact optimal solution to this cardinality minimization problem. The proposed result is based on a polyhedral combinatorics argument. It is different from well-known results based on mutual coherence and restricted isometry property. The results are illustrated on benchmarks including the IEEE 118-bus, IEEE 300-bus, and the Polish 2383-bus and 2736-bus systems.

C. W. Ten, G. Manimaran and C. C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," in *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853-865, July 2010.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5477189&isnumber=5484919

Disruption of electric power operations can be catastrophic on national security and the economy. Due to the complexity of widely dispersed assets and the interdependences among computer, communication, and power infrastructures, the requirement to meet security and quality compliance on operations is a challenging issue. In recent years, the North American Electric Reliability Corporation (NERC) established a cybersecurity standard that requires utilities' compliance on cybersecurity of control systems. This standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices). In this paper, a comprehensive survey on cybersecurity of critical infrastructures is reported. A supervisory control and data acquisition security framework with the following four major components is proposed: 1) real-time monitoring; 2) anomaly detection; 3) impact analysis; and 4) mitigation strategies. In addition, an attack-tree-based methodology for impact analysis is developed. The attack-tree formulation based on power system control networks is used to evaluate system-, scenario-, and leaf-level vulnerabilities by identifying the system's adversary objectives. The leaf vulnerability is fundamental to the methodology that involves port auditing or password strength evaluation. The measure of vulnerabilities in the power system control framework is determined based on existing cybersecurity conditions, and then, the vulnerability indices are evaluated.

C. Vellaithurai, A. Srivastava, S. Zonouz and R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," in *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566-575, March 2015.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6979242&isnumber=7042857

To protect complex power-grid control networks, power operators need efficient security assessment techniques that take into account both cyber side and the power side of the

cyber-physical critical infrastructures. In this paper, we present CPINDEX, a security-oriented stochastic risk management technique that calculates cyber-physical security indices to measure the security level of the underlying cyber-physical setting. CPINDEX installs appropriate cyber-side instrumentation probes on individual host systems to dynamically capture and profile low-level system activities such as inter process communications among operating system assets. CPINDEX uses the generated logs along with the topological information about the power network configuration to build stochastic Bayesian network models of the whole cyber-physical infrastructure and update them dynamically based on the current state of the underlying power system. Finally, CPINDEX implements belief propagation algorithms on the created stochastic models combined with a novel graph-theoretic power system indexing algorithm to calculate the cyber-physical index, i.e., to measure the security-level of the system's current cyber-physical state. The results of our experiments with actual attacks against a real-world power control network shows that CPINDEX, within few seconds, can efficiently compute the numerical indices during the attack that indicate the progressing malicious attack correctly.

J. Wan, A. Canedo and M. A. Al Faruque, "Security-aware functional modeling of Cyber-Physical Systems," *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1-4.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7301644&isnumber=7301399

Security is one of the major challenges for Cyber-Physical Systems (CPS) design. Identifying flaws as early as possible in the CPS design saves time and money; between 5_ to 10_ less expensive than finding them during the detailed design stages. This paper makes a case for finding cybersecurity flaws as early as possible. Not only for the temporal and cost benefits, but more importantly, for the integrity of the system once in operation. We introduce a security-aware functional modeling methodology, supported by simulation to validate the robustness of the system in the presence of attacks and countermeasures. Our ideas are implemented in a design automation tool in Amesim and Matlab/Simulink. We use an automotive use-case as an example to validate the methodology and the tool.

G. A. Weaver *et al.*, "Cyber-Physical models for power grid security analysis: 8-substation case," *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, NSW, 2016, pp. 140-146.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7778752&isnumber=7778724

Utilities need to understand and consider the interconnectedness of their electrical system and its supporting cyber infrastructure to maintain system reliability in the face of cyber adversaries. This paper makes two contributions to modeling cyber-physical dependencies within the electrical power sector. First, the paper defines a Common Format using the Cyber- Physical Topology Language (CPTL) to inventory, analyze, and exchange cyber-physical model information. Second, the paper provides an 8-substation cyber-physical reference model. The impact of this work is to enable efficient

information exchange of cyber-physical topologies within and among the industry as well as the research community. The reference model and framework will benefit the research community by providing a way to compare analyses on electrical power systems that account for problems within cyber control networks.

W. Wu, R. Kang and Z. Li, "Risk assessment method for cyber security of cyber physical systems," *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, Beijing, 2015, pp. 1-5.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7366430&isnumber=7366393

Cyber security is one of the most important risks for all types of cyber–physical systems (CPS). To evaluate the cyber security risk of CPS, a quantitative hierarchized assessment model consists of attack severity, attack success probability and attack consequence is proposed, which can assess the risk caused by an ongoing attack at host level and system level. Then the definitions and calculation methods of the three indexes are discussed in detail. Finally, this paper gives the risk assessment algorithm which describes the steps of implementation. Numerical example shows that the model can response to the attack timely and obtain the system security risk change curve. So that it can help users response to the risk timely. The risk change curve can also be used to predict the risk for the future time.

S. Yoneda, S. Tanimoto, T. Konosu, H. Sato and A. Kanai, "Risk Assessment in Cyber-Physical System in Office Environment," *2015 18th International Conference on Network-Based Information Systems*, Taipei, 2015, pp. 412-417.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7350652&isnumber=7350553

The Internet and mobile communications have become more important pieces of infrastructure. On the other hand, the security incidents about an information security have increased in proportion to the spread of the Internet and mobile communications. Thus, confidential information needs to be protected strictly from these threats. Specifically, the view of the security management that also considers both physical and information security, i.e., security of cyber-physical systems, is becoming important. This paper describes the risk assessment in a cyber-physical system for the office of an enterprise from the viewpoint of a user. That is, risk assessment of the cyber-physical system in the office based on the viewpoint of a user is clarified.

Y. Zhang, L. Wang, Y. Xiang and C. W. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," in *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707-1721, July 2015.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7042739&isnumber=7128463

As information and communication networks are highly interconnected with the power grid, cyber security of the supervisory control and data acquisition (SCADA) system has become a critical issue in the electric power sector. By exploiting the vulnerabilities in cyber components and intruding into the local area networks of the control center,

corporation, substations, or by injecting false information into communication links, the attackers are able to eavesdrop critical data, reconfigure devices, and send trip commands to the intelligent electronic devices that control the system breakers. Reliability of the power system can thus be impacted by various cyber attacks. In this paper, four attack scenarios for cyber components in networks of the SCADA system are considered, which may trip breakers of physical components. Two Bayesian attack graph models are built to illustrate the attack procedures and to evaluate the probabilities of successful cyber attacks. A mean time-to-compromise model is modified and adopted considering the known and zero-day vulnerabilities on the cyber components, and the frequencies of intrusions through various paths are estimated. With increased breaker trips resulting from the cyber attacks, the loss of load probabilities in the IEEE reliability test system 79 are estimated. The simulation results demonstrate that the power system becomes less reliable as the frequency of successful attacks on the cyber components increases and the skill levels of attackers increase.

T. Zhi, G. Si, X. He and Y. Xu, "Simulation Model of Cascading Effects from Cyber Attacks on Electric Power Infrastructure Networks," *2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, Beijing, 2011, pp. 996-999.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6154277&isnumber=6119178

To destroy a country's physical electric power infrastructure by attacking its control system through cyber means, has become an important way to weaken a country's war power. Along with the construction of next generation smart grid, development of the internet of things and appearance of system of systems(henceforth, SOS) warfare based on information systems, the complicated control networks system would confront more and more threat of cyber attack. we design the main structure and key arithmetic of the model, based on the physical electric power infrastructure whose cyber and physical system is close interdependent in order to provide theoretic reference to the analyzing and evaluating the cascading effects from increasing cyber attack to physic system. Preliminary experiments show that these structures and algorithms are reasonable and feasible.

Mission Assurance

L. Buchanan, M. Larkin and A. D'Amico, "Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users," *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2012, pp. 298-304.

http://ieeexplore.ieee.org/document/6459865/

Decision makers must know if their cyber assets are ready to execute critical missions and business processes. Net-work operators need to know who relies on a failed network asset (e.g. IP address, network service, application) and what critical operations are impacted. This requires a mapping between net-work assets and the critical operations that depend on them, currently a manual and tedious task. In addition, because of the

dynamic nature of networks and missions, manual mappings of network assets to operational missions rapidly become outdated. This paper describes one approach to modeling the complex relationships between cyber assets and the missions and users that depend on them, using an ontology developed in conjunction with practitioners and cyber mission assurance researchers. We describe the "Camus" (cyber assets, missions and users) proof of concept, which uses this ontology and automatically populates that model from data already on the network. We discuss the technical approach and provide examples of query results re-turned by the model. We conclude by describing ongoing work to enhance this proof of concept and its potential applicability to support mission assurance and mission impact solutions.

Guariniello, C. & DeLaurentis, D., (2014). Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. CSER.

https://doi.org/10.1016/j.procs.2014.03.086

The analysis of risks associated with communications, and information security for a system-of-systems is a challenging endeavor. This difficulty is due to the complex interdependencies that exist in the communication and operational dimensions of the system-of-systems network, where disruptions on nodes and links can give rise to cascading failure modes. In this paper, we propose the modification of a functional dependency analysis tool, as a means of analyzing system-of-system operational and communication architectures. The goal of this research is to quantify the impact of attacks on communications, and information flows on the operability of the component systems, and to evaluate and compare different architectures with respect to their reliability and robustness under attack. Based on the topology of the network, and on the properties of the dependencies, our method quantifies the operability of each system as a function of the availability and correctness of the required input, and of the operability of the other systems in the network. The model accounts for partial capabilities and partial degradation. Robustness of the system-of-systems is evaluated in terms of its capability to maintain an adequate level of operability following a disruption in communications. Hence, different architectures can be compared based on their sensitivity to attacks, and the method can be used to guide decision both in architecting the system-of-systems and in planning updates and modifications, accounting for the impact of interdependencies on the robustness of the system-of-systems. Synthetic examples show conceptual application of the method.

G. Hastings, L. Montella, J. Watters, "MITRE Crown Jewels Analysis Process", *The MITRE Corporation MTR 090088*, April 2009.

https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

Crown Jewels Analysis (CJA) is a process for identifying those cyber assets that are most critical to the accomplishment of an organization's mission. CJA is also an informal name for Mission-Based Critical Information Technology (IT) Asset Identification. It is a subset of broader analyses that identify all types of mission-critical assets.

D. Henshel *et al*., "Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification," *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2016, pp. 1-5.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7568937&isnumber=7568873

Decision-making in cyber-security is mostly ad-hoc and highly reliant on static policies, as well as human intervention. This does not fit current networks/systems, as they are highly dynamic systems where security assessments have to be performed, and decisions have to be made, automatically and in real-time. To address this problem, we propose a risk-based approach to cybersecurity decision-making. In our model, the system undergoes a continuous security risk assessment based on risk; decisions for each action are taken based on constructing a sequence of alternative actions and weighing the cost-benefit trade-offs for each alternative. We demonstrate the utility of our system on a concrete example involving protecting an SQL server from SQL injection attacks. We also discuss the challenges associated with implementing our model.

K. Jabbour, S. Muccio, 2011. The Science of Mission Assurance, Journal of Strategic Security 4, no. 2, pp. 61-74.

http://scholarcommons.usf.edu/jss/vol4/iss2/5

The intent of this article is to describe—and prescribe—a scientific framework for assuring mission essential functions in a contested cyber environment. Such a framework has profound national security implications as the American military increasingly depends on cyberspace to execute critical mission sets. In setting forth this prescribed course of action, the article will first decompose information systems into atomic processes that manipulate information at all six phases of the information lifecycle, then systematically define the mathematical rules that govern mission assurance.

G. Jakobson, 2011. Mission Cyber Security Situation Assessment Using Impact Dependency Graphs, Proceedings of the 14th International Conference on Information Fusion, Chicago, IL.

http://ieeexplore.ieee.org/document/5977648/

The paper proposes a conceptual framework and a method for assessing impact that cyber attacks might have to cyber assets, services, and missions. The paper describes the model of a cyber attack based on an extended conceptual graph. It introduces the notion of a cyber-terrain as a multilevel information structure containing assets and services, and their inter-dependencies. It also describes the model of a mission, and impact dependency graph that in a uniform way presents the dependencies between the cyber terrain and missions. The paper presents an algorithmic base how to calculate impacts that cyber attacks cause to the directly attacked assets, how the direct impacts propagate through the interasset, service, and mission dependencies and affect the operational capacity of ongoing missions.

G. Jakobson, "Mission-centricity in cyber security: Architecting cyber attack resilient missions," *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, 2013, pp. 1-18.

http://ieeexplore.ieee.org/document/6568387/

Until recently the information technology (IT)-centricity was the prevailing paradigm in cyber security that was organized around confidentiality, integrity and availability of IT assets. Despite of its widespread usage, the weakness of IT-centric cyber security became increasingly obvious with the deployment of very large IT infrastructures and introduction of highly mobile tactical missions where the IT-centric cyber security was not able to take into account the dynamics of time and space bound behavior of missions and changes in their operational context. In this paper we will show that the move from IT-centricity towards to the notion of cyber attack resilient missions opens new opportunities in achieving the completion of mission goals even if the IT assets and services that are supporting the missions are under cyber attacks. The paper discusses several fundamental architectural principles of achieving cyber attack resilience of missions, including mission-centricity, survivability through adaptation, synergistic mission C2 and mission cyber security management, and the real-time temporal execution of the mission tasks. In order to achieve the overall system resilience and survivability under a cyber attack, both, the missions and the IT infrastructure are considered as two interacting adaptable multi-agent systems. While the paper is mostly concerned with the architectural principles of achieving cyber attack resilient missions, several models and algorithms that support resilience of missions are discussed in fairly detailed manner.

T. Llansó, P. A. Hamilton and M. Silberglitt, "MAAP: Mission Assurance Analytics Platform," *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2012, pp. 549-555.

http://ieeexplore.ieee.org/document/6459908/

This paper describes the Mission Assurance Analytics Platform (MAAP), an open, experimental software framework that provides analysts with an environment for systematically studying the link between cyber attack and the resulting impact on operational missions that are supported by a cyber system. MAAP directly informs both risk decisions and mitigation prioritization.

T. Llansó and E. Klatt, "CyMRisk: An approach for computing mission risk due to cyber attacks," *2014 IEEE International Systems Conference Proceedings*, Ottawa, ON, 2014, pp. 1-7.

http://ieeexplore.ieee.org/document/6819227

This paper provides an overview of CyMRisk, an experimental architecture for computing mission risk due to cyber attack. In its current form, the approach employs a simulation of key aspects of a target business/mission process as well as attacker behavior to estimate mission impact due to cyber attacks. In addition, CyMRisk estimates worst case attacker level of effort associated with carrying out such attacks.

T. Llansó, A. Dwivedi, M. Smeltzer, "An approach for estimating cyber attack level of effort", Systems Conference (SysCon) 2015 9th Annual IEEE International, pp. 14-19, 2015.

http://ieeexplore.ieee.org/document/7116722

Timely risk assessments allow organizations to gauge the degree to which cyber attacks threaten their mission/business objectives. Risk plots in such assessments typically include cyber attack likelihood values along with the impact. This paper describes an algorithm and an associated model that allow for estimation of one aspect of cyber attack likelihood, attack level of effort. The approach involves the use of an ordinal set of standardized attacker tiers, associated attacker capabilities, and protections (security controls) required to resist those capabilities.

M. Monteiro, T. Sarmento, A. Barreto, P. Costa, M. Hieb, "An integrated mission and cyber simulation for Air Traffic Control", *Intelligent Transportation Systems (ITSC) 2016 IEEE 19th International Conference on*, pp. 2687-2692.

http://ieeexplore.ieee.org/document/7795988

Worldwide statistics show that air traffic has been growing significantly in recent years. In order to maintain safety, new technologies and architectures are constantly being proposed and deployed. However, several of those technologies contain design flaws and security vulnerabilities which, if properly exploited, can affect the Air Traffic Control (ATC) system in such a way that its effects could range from simple flight delays (economic loss) to air disasters (loss of life). In order to better assess the new generation of air traffic services, this paper presents a simulation/emulation framework based on open source tools to able to evaluate the effects of cyber-attacks and network/communication failures on Air Traffic Control. It presents a case study on Automatic Dependent Surveillance - Broadcast (ADS-B) technology, with real implementations of cyber-attacks at the link layer. Furthermore, mitigation/defense mechanisms are also evaluated from a mission-assurance perspective.

S. Musman, A. Temin, M. Tanner, D. Fox, B. Pridemore, 2009. Evaluating the Impact of Cyber Attacks on Missions, the MITRE Corp.

Also available as S. Musman A. Temin M. Tanner R. Fox B. Pridemore "Evaluating the impact of cyber attacks on missions" Proceedings of the 5th International Conference on Information Warfare and Security pp. 446-456 2010.

http://www.mitre.org/sites/default/files/pdf/09_4577.pdf

Using current methods, it is virtually impossible to determine the impact of a cyber attack on the attainment of mission objectives. Do we know which mission elements are affected? Can we continue to operate and fulfill the mission? Should we wait for recovery? Can we salvage part of the mission? Since it is currently so difficult for humans to comprehend the mission impact of a cyber incident, our ability to respond is much less effective than it could be. We believe that improved knowledge of the mission

impact of a cyber attack will lead to improved, more targeted responses, creating more attack resistant systems that can operate through cyber attacks.

Our work addresses the "mission" part of "mission assurance," focusing on cyber mission impact assessment (CMIA). Our challenge is to create mission models that can link information technology (IT) capabilities to an organization's business processes associated with Measures of Effectiveness and Performance (e.g., attrition of enemy forces , targets destroyed, blue force protection). Measuring mission impact requires knowing the mission activities that fulfill mission needs, the supporting cyber assets, and understanding how the effects of an attack change mission capability. This paper is about developing the techniques that make estimating the mission impact of cyber attacks possible.

S. Musman, M. Tanner, A. Temin, E. Elsaesser and L. Loren, "A systems engineering approach for crown jewels estimation and mission assurance decision making," *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, Paris, 2011, pp. 210-216.

http://ieeexplore.ieee.org/document/5949403

Understanding the context of how IT contributes to making missions more or less successful is a cornerstone of mission assurance. This paper describes a continuation of our previous work that used process modeling to allow us to estimate the impact of cyber incidents on missions. In our previous work we focused on developing a capability that could work as an online process to estimate the impacts of incidents that are discovered and reported. In this paper we focus instead on how our techniques and approach to mission modeling and computing assessments with the model can be used offline to help support mission assurance engineering. The heart of our approach involves using a process model of the system that can be run as an executable simulation to estimate mission outcomes. These models not only contain information about the mission activities, but also contain attributes of the process itself and the context in which the system operates. They serve as a probabilistic model and stochastic simulation of the system itself. Our contributions to this process modeling approach have been the addition of IT activity models that document in the model how various mission activities depend on IT supported processes and the ability to relate how the capabilities of the IT can affect the mission outcomes. Here we demonstrate how it is possible to evaluate the mission model offline and compute characteristics of the system that reflect its mission assurance properties. Using the models it is possible to identify the crown jewels, to expose the systems susceptibility to different attack effects, and evaluate how different mitigation techniques would likely work. Being based on an executable model of the system itself, our approach is much more powerful than a static assessment. Being based on business process modeling, and since business process analysis is becoming popular as a systems engineering tool, we also hope our approach will push mission assurance analysis tasks into a framework that allows them to become a standard systems engineering practice rather than the "off to the side" activity it currently is.

S. Musman, M. Tanner, A. Temin, E. Elsaesser and L. Loren, "Computing the impact of cyber attacks on complex missions," *2011 IEEE International Systems Conference*, Montreal, QC, 2011, pp. 46-51.

http://ieeexplore.ieee.org/document/5929055

This paper describes how to evaluate the impact of a cyber attack on a mission. We accomplish this by computing impact as the changes to mission measures of effectiveness, based on the reported effects of a known or suspected attack on one or more parts of the information technology (IT) supporting the mission. Our previous papers have described our goals for computing mission impact and the choices of the techniques we use for modeling missions, IT, and cyber attacks. This paper focuses on how we compute the impact of cyber attacks on IT processes and information. These computations will improve decision-making when under cyber attack by providing accurate and detailed assessments of the impact of those attacks. Although the focus of our work has been on the calculation of cyber mission impacts during mission execution, we have also demonstrated how our representations and computations can be used for performing cyber risk analysis and crown jewels analysis.

S. Musman, A. Temin, "A Cyber Mission Impact assessment tool", *Technologies for Homeland Security (HST) 2015 IEEE International Symposium on*, pp. 1-7, 2015.

http://ieeexplore.ieee.org/document/7225283

The promise of practicing mission assurance is to be able to leverage an understanding of how mission objectives and outcomes are dependent on supporting cyber resources. This makes it possible to analyze, monitor, and manage your cyber resources in a mission context. In previous work, we demonstrated how process modeling tools can simulate mission systems to allow us to dynamically compute the mission impacts of cyber events. We demonstrated the value of using this approach, but unfortunately practical deployment of our work was hampered by limitations of existing commercial off-the-shelf (COTS) tools for process modeling. To address this deficiency, we have developed our own Cyber Mission Impact Business Process Modeling tool. Although it implements only a functional subset of the business process modeling notation (BPMN), it has, unlike the more generic COTS tools, been specifically designed for the representation of cyber processes, resources, and cyber incident effects. The method and tool are described in this paper.

S. Musman, "Assessing prescriptive improvements to a system's cyber security and resilience", *Systems Conference (SysCon) 2016 Annual IEEE*, pp. 1-6, 2016.

http://ieeexplore.ieee.org/document/7490660

In the process of creating new capabilities, and improving the efficiency of existing operational processes, as a society, we have become dependent on information and communications technology (ICT). ICT is now integral to almost every aspect of our daily activities. The detrimental impact of these ICT dependencies, however, is that business operations become susceptible to possible impacts from cyber incidents.

Protecting ICT from cyber incident effects or reducing their impacts on operational activities has become a problem of national importance. Concomitantly, there is an escalating imperative to identify and minimize operational cyber risk. In almost all circumstances, we are interested in achieving operational resilience: the ability for systems to continue to fulfil their intended purpose in the face of actual or potential cyber incidents. Achieving such resilience almost always must be pursued in a resource limited environment, where there is a need to justify the costs and resources needed. Unfortunately most current definitions of resilience are qualitative ones. If resilience is defined in a qualitative rather than quantitative way there is little in the way of prescriptive advice that can be offered to increase resilience. To address this deficiency we use a quantitative definition of resilience and apply it in a game theory inspired approach that considers multiple cyber attacker moves ahead. This allows us to assess defender actions as a portfolio analysis to identify a prescriptive selection of the best employment of security and resilience methods to use.

Y. Naudet, N. Mayer and C. Feltus, "Towards a Systemic Approach for Information Security Risk Management," *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, 2016, pp. 177-186.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7784568&isnumber=7784494

Risk management in the field of information security is most often handled individually by enterprises, taking only a limited view on the influential factors coming from their providers, clients or more globally from their environment. This approach becomes less appropriate in the case of networked enterprises, which tend to form ecosystems with complex influence links. A more holistic approach is needed to take these into account, leading to systemic risk management, i.e. risk management on the entire system formed by the networked enterprises, to avoid perturbations of the ecosystem due to local, individual, decision-making. In this paper, we propose a new meta-model for Information System Security Risk Management (ISSRM), comprising systemic elements as defined in the General Systems Theory. We discuss the design of this new model, highlighting in particular how risk management can be related to a problem-solving approach and the important concepts that are instantiated when taking a systemic approach to ISSRM.

S. Naumov and I. Kabanov, "Dynamic framework for assessing cyber security risks in a changing environment," *2016 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, 2016, pp. 1-4.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7777406&isnumber=7777371

Cyber risk assessment frameworks aim at addressing a challenging problem that public and commercial organizations and nations embrace today - a proper estimation of likelihood of cyber-related risks and assessment of their potential impact on an enterprise. However, current frameworks fail at adapting to changes which happen in dynamically shifting environments and keep organizations blind to new possible threats. These threats may occur because of different changes happening internally or externally of the organization. For example, the global presence or digital footprint of the organization can

significantly increase the exposure of an organization to cyber threats. Therefore, practitioners need new instruments which can be used to advise enterprises when and how their risk assessment methods and processes should be adjusted in order to stay relevant in a rapidly changing environment. In this work, the authors propose and validate a new method of applying a system dynamics approach for designing a dynamic risk assessment framework and introduce areas of future work.

D. Ormrod, B. Turnbull and K. O'Sullivan, "System of systems cyber effects simulation ontology," *2015 Winter Simulation Conference (WSC)*, Huntington Beach, CA, 2015, pp. 2475-2486.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7408358&isnumber=7408148

This paper outlines the requirements for a series of ontologies necessary to provide a meaningful answer to the question: How do we model and simulate the System of Systems effects of a cyber attack on an organization or military unit? This work provides the data model specification for a simulation to answer this question by explaining the required domains of knowledge. We introduce mechanisms to federate these domains, and then provide an exemplar use-case to contextualize one type of scenario the model must be capable of representing within a simulation environment. The model demonstrates the granularity necessary for the modeling and simulation of a SoS effect of a cyber attack on an organization or military unit.

M. Pritchett, 2012. Cyber Mission Assurance: A Guide To Reducing The Uncertainties Of Operating In A Contested Cyber Environment, MS Thesis, Air Force Institute of Technology.

http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA563712

Military organizations have embedded Information and Communication Technology (ICT), collectively known as “Cyberspace,” into their core operational processes across all levels of military operations. Cyber mission assurance is an essential risk management activity focused on assuring an organization’s mission capability in response to any loss or degradation of cyber capabilities. The cyber mission assurance process requires an in depth analysis of the organization’s mission including enumeration of its core mission processes, prioritization of mission processes, mapping of mission processes to underlying cyber capabilities, and application of control measures to mitigate risks to mission capability. Unfortunately, the structure of military organizations makes this type of analysis challenging as the mission tasks and cyber ICT capabilities virtually always span multiple organizational boundaries.

The 24th Air Force recently developed new draft guidance for conducting cyber mission assurance, 24th Air Force & 624th Operations Center Mission Assurance Operating Concept, 2011. The goal of this research is to present a methodology enabling mission owners to efficiently prepare for cooperative cyber mission assurance engagements with 24th Air Force. The proposed methodology incorporates the new 24th Air Force guidance; best practices from commercial, governmental, and military organizations; and

incorporates operational lessons learned. Application of the proposed methodology will enable more efficient and productive cyber mission assurance engagements with 24th Air Force.

Sun, T. Y. Wu, X. Liu and M. S. Obaidat, "Multilayered Impact Evaluation Model for Attacking Missions," in *IEEE Systems Journal*, vol. 10, no. 4, pp. 1304-1315, Dec. 2016.

http://ieeexplore.ieee.org/document/6898814/

In practical application scenarios, direct attacking on a target system to test the impact of attack methods may expose an attacker's intent and result in the difficulty in evaluating the attack method. Therefore, it is essential to design a controllable target range for testing and evaluating the attack impact. In this paper, we construct an attack test platform in order to evaluate the attack impact from different attack tools or the combinations of these attack tools. According to “vulnerability-asset-service-mission” (VASM) relationship, we design a multilayered evaluation model VASM, which includes a four-layer information structure: vulnerability layer, asset layer, service layer, and mission layer, from bottom to top. Considering that each asset may have one or more vulnerabilities, we score the attack impact on each asset based on attack probability and vulnerability and calculate the operational capacity of an asset after an attack. Since services may be provided jointly by one or more assets, we calculate the attack impact on services utilizing the dependencies among assets. The attack impact can be transmitted layer by layer from bottom to top through the dependencies among nodes. Finally, we can obtain the attack impact on missions. We use an actual logistics management and tracking system as the target range and verify the effectiveness and validity of our evaluation model, i.e., VASM, on goods delivery. Experimental results show that VASM cannot only assess the attack impact directly but also conform to the actual situations accurately.

This page intentionally left blank.

DISTRIBUTION

2 Department of Homeland Security Office of Cyber and Infrastructure Analysis
Attn: K. Kilby, R. Hanson
NPPD/OCIA
245 Murray Lane, M/S 0390
Washington DC 20528-0390

1	MS1138	Nancy Brodsky	8873
1	MS1138	Rossitza Homan	8815
1	MS0899	Technical Library	9536 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories