NOTE:The following paper is in rough draft. We are seeking feedback on the logic, flow and completeness of the paper. A companion powerpoint is also attached for additional information. For the most recent version prior to the talk, the paper is on google drive at: https://docs.google.com/document/d/1F9rSreFyeTdUZF0uF1CNYv49-4688817OZan3V7_oTs/edit?usp=sharing

Integrating Attackers and Defender into Cyber Security Risk Models

Diane Henshel, Alexander Alexeev, Mariana Cains, Varun Agarwal
Indiana University

Blaine Hoffman
Army Research Lab

Abstract - Current approaches to modeling cyber security risk assessment typically only include assets, the hardware and software of a cyber network, especially those based on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Cyber security risk modeling methodologies which are currently utilised by tech industries and government agencies do not consider humans as risk initiators or mitigators. Human factors are considered primarily in terms of how users use networks, which help defenders and IT managers prioritize assets; while the defenders and IT managers consider risk from their perspective of how to best protect their system. Risk management within the context of the NIST framework does not consider humans as actual risk factors, initiators and mitigators of risk, and therefore potential components of a predictive model of network security risk. Attributes of the human actors, attackers, defenders, and users, such as experience, knowledge and cultural background, may significantly influence how human actors contribute to or mitigate cyber risk, and thus are appropriate parameters to include in a predictive cyber security risk model. In this paper, we extend our previous work conceptualizing a dynamic aggregated cybersecurity risk assessment model based on a Bayesian belief network and incorporate variables representing critical risk-inducing and risk-mitigating human and cultural factors into a proof of concept. We introduce human factor parameters to incorporate attacker and defender skills into our modeling framework and integrate a country-based modifying threat factor. We use empirical distributions for the nodes in the Bayesian network, adapted from data observed and documented by studies of SQL injection attacks. Using empirical evidence gives a more versed view of how changes in the network affect the overall risk, in comparison to using theoretical assumptions. We discuss how including human factors contribute to altering risk in cyber networks, detailing the potential impacts and effects of human actors on risk posture, strategy, and response. We model and evaluate the risks for an SQL injection attack on a highly sensitive database server. We will discuss parametrization and validation of the model using empirical data obtained in the experiment on a virtual network test bed.

Highlights:

Keywords:
Abbreviations:

1. Introduction.

Widely used cyber security risk frameworks, especially the NIST Framework for Improving Critical Infrastructure Cybersecurity, list guidelines and good practices to achieve a reasonable level of risk management strategy for an organization. Although the NIST framework does not claim to provide an exhaustive list of risk categories to be considered while assessing risk for an organization, the framework does not incorporate the risk posed by human factors.

We expand on our previous work where we presented a holistic risk framework to calculate cyber security risk dynamically. In this paper, we focus on human factors as potentially necessary components of a holistic cyber security framework, and present the Multi-Level Risk Assessment Parametrization (MulRAP) framework used to systematically characterize the network being modeled and identify the most important risk assessment model metrics. The utility of the MulRAP framework to identify crucial risk metrics and the inclusion of human factors in a risk assessment model is exemplified in a Bayesian network. The model presented in this paper features attackers and defenders as separate human entities, and includes them as distinct nodes in the Bayesian network. This paper thus presents a different perspective compared to existing cyber security risk frameworks, which do not incorporate human attackers and defenders as potential risk modifiers.

The bayesian network model presented in this paper is not meant to fit the risk modeling requirements of a particular organization. Each organization has its own definition of risk, and requires the framework to be molded according to the cybersecurity needs of the organization. The model only serves to support the risk modeling approach and the framework that is presented in the paper, and suggests how cultural and human factors could be integrated into a cybersecurity risk model.

- To incorporate human factors (attackers and defenders) into existing cyber security risk models.
- To incorporate national culture as a modifying threat factor into the cybersecurity model.
- To quantify risk by modeling it dynamically, in this instantiation using a database server SQL attack model.
- To identify the minimum number of necessary and sufficient risk metrics that capture the dynamic system risk.
- To observe how risk is dependent on the provenance of the SQL request.

The rest of this paper is organized as follows...

2. Cyber systems as complex systems

Cyber systems are inherently complex systems. Complex systems are characterized by having many components often linked through hierarchical, serial, and parallel relationships exhibiting feedback and feedforward interactions in addition to classical cause and effect interactions [1,2,3]. Data in multiscale systems are often collected at different scales within the system and in disparate units of measurement which need to be integrated across scales and units into a single model or set of simultaneous equations. A major complexity in cyber systems is the humans. Humans use and interact with cyber systems, protect and manage cyber systems, and purposely interfere with cyber systems (as attackers, or just to get around blocks that the humans perceive as unwanted). Humans are integral parts of most cyber systems, affecting

both function and risk, yet there is a paucity of quantified data about how to integrate "humans in the loop" when modeling cyber systems. Additionally, time- and state-dependent changes need to be integrated in order to model dynamic systems that change over time, especially when system function, or the mission, requires the accurate completion of specific sequential tasks and subtasks. The transmission of a Wi-Fi signal sent by a router requires the completion of integrated actions at the sub-router level (a different scale), such as the timely processing by multiple chips in the router integrated in sequence (serial action) or in a combination of serial and parallel processes. Yet another problem with complex systems is that the actions of some assets may be measured or quantified on a continuous scale, while the actions of other assets must be quantified on a discrete scale (e.g. binomial: go/no go). The actions of other assets are difficult to measure at all, either due to technical/logistic complications (the change that occurs is too fast to measure at the operating temperature) or is difficult to observe frequently enough to get statistically robust estimates. In addition, bias and uncertainty in observation, measurement, and analysis need to be accounted for, if not adjusted for.

In sum, modeling risk in complex systems faces the following difficulties: 1) the need to combine metrics that are determined using very different units, 2) the need to combine metrics that exist at multiple scales, 3) the need to model serial risks that are introduced due to serial interactions within the system or that "ripple out" from the initial system stressor; 4) the need to adjust for dynamic interactions in the system that alter the system itself as well as altering the risk in the system; 5) the need to incorporate multiple types of metrics in the model, including some that are primary risk (types of impact) metrics, some that are magnitude metrics, and some that only contribute a weighting value to other metrics. The ideal approach to modeling risk in a complex, dynamic system (such as the changing vulnerabilities in a cyber network) would be to calculate the risk as a "living process," responsive to the current state of the system and capable of recalculation when new data is available (new detection data) or when the system state has changed. The standard engineering approach to risk assessment has been to simplify first and then slowly integrate complexity into the system. The NIST guidelines recognize that risk management is an iterative process of risk identification, risk assessment, and risk mitigation [4,5]. However the iterative cycling is in the order of years and thus considers risk statically and does not take state changes into account.

In its simplest form, risk assessment is a decision-making tool that quantifies (or semi-quantifies) the likelihood and impact of an event of concern. Traditional risk assessments perform a baseline assessment calculating the impact of a single threat on a single event, however such assessments are not representative of the complex systems and relationships in the physical world nor the cyber realm. Risk assessments for a single threat and single event in a simple, one operational asset system are easily organized into a simplified causal chain of source of threat, point of vulnerability, exploitation of vulnerability, and event impact. This method of organization does not capture the hierarchical nor parallel relationships that characterize and define a complex system. In an effort to advance the science of cybersecurity risk assessment, we present a method for organizing the framing of complex systems in order to identify system components that are critical to addressing the risk management question, and how humans factors (attackers and defenders) can be included in risk assessment models.

3. Rationale for the Multi-Level Risk Assessment Parameterization Framework

3.1 Framing (Problem formulation)

The current state of cybersecurity risk assessment is formalized in the NIST cybersecurity risk assessment framework and risk management guidances [4,5]. The NIST guidelines emphasize that risk management is an iterative process, recognizing that, in practice, the iterations are infrequent. The NIST cybersecurity framework provides the following structure for conducting a risk assessment through five functions [5]: 1) Identify the organizational structure and assets relevant to cybersecurity infrastructure assets and services; 2) Protect critical cybersecurity infrastructure services with appropriate safeguards; 3) Detect cybersecurity threats and anomalous events; 4) Respond to detected cybersecurity events; and 5) Recover and restore impaired organizational assets and services (Figure 1). The Identify function is central for effective use of the NIST framework; currently, however, no organizational schema exists that sufficiently reflects the complex relationships within military cyber infrastructure assets and services. We have developed two frameworks to facilitate the framing and execution of quantitative cybersecurity risk assessments. First, the Holistic Cybersecurity Risk Assessment (HCRA) Framework was developed by adapting and extending established decision-making methodologies. The Observe-Orient- Decide-Act (OODA) Loop developed by USAF Colonel John Boyd [6; see Figure 2], the Presidential/Congressional Commission on Risk Assessment and Risk Management's Framework for Environmental Health Risk Management (FEHRM) [7, see Figure 3], and the 2017 NIST Cybersecurity Framework Core [5, Figure 1] were integrated together to produce the HCRA Framework (see Figure 4). This framework outlines the iterative higher level steps necessary to identify, assess, and respond to potential and known cybersecurity threats.

3.2 Parameterization issues for complex systems: identifying key (necessary and sufficient) metrics quantifying / qualifying relationships between metrics. (developing indicators and indices, performance measures)

3.3 Risk Assessment Modeling of Complex Systems

Complex systems pose another challenge, in terms of identifying and modeling the risk associated with them. Alongside the fact that their behavior is non-linear, it is also dynamic in nature. The dynamic nature of cyber systems is due to the variability of their interaction with humans and other cyber systems. Attackers adapt to the advancements made in web security technologies, and defenders adapt to new types of attacks to develop better web security measures. Moreover, interaction of end users with systems introduces a dynamic component to cyber risk assessment, due to the different end goals, usage mannerisms, access levels and roles, which can change over time. [Modeling Cybersecurity Risks, Henshel et al, 2016) mentions that system state changes with the most recent activity in the system. Building on this, we believe that system risk should be assessed dynamically,

In this paper, we promulgate the notion of assessing risk dynamically in time, through the combination of

the MulRAP Framework and the Bayesian network approach to modeling risk. The bayesian network we have built responds to every incoming connection request to a database server, with the database as the main asset in the mission whose risk is to be assessed. The MulRAP Framework helps identify parameters which explain the dynamic nature of such systems, and the nature of Bayesian networks makes it suitable to model dynamic system risk.

(1. Talk about why static calculation of risk is not appropriate, and how calculating risk dynamically trumps static calculation
2. Talk about the approach we use in our modeling of risk)

2.1 Humans as variables and risk factors in cybersecurity risk assessment models

Humans are integral to any cyber network. Attackers and defenders in cybersecurity are generally studied independent of other risk factors in a cyber network. [Roy et al 2010] studies the behavior of attackers and possible defense mechanisms using Attack Countermeasure Trees (ACT), which is an adaptation of attack trees which are widely used to study attackers in a cyber network. [Mc Queen, et al 2006] presents a quantitative cyber risk reduction estimation methodology by modeling time-to-compromise as a function of known vulnerabilities in the system and attacker skill level. It estimates dominant attack paths to identify the paths with maximum risk. As such, human metrics as risk altering factors in a cyber network are generally analyzed independent of other risk metrics that affect the overall risk in a cyber network. They are mostly studied in the form of attack trees or blue versus red (defender versus attacker) game theory based security models.

2.2 National cultural factors in cybersecurity risk models

Additionally, cultural factors have been identified to substantially affect the behavior of attackers, defenders, and users in a cyber security scenario. [Henshel et al 2016a] discusses the importance of cultural factors that affect the behavioral characteristics of humans and their interactions within a cybersecurity risk framework. It addresses the importance of culture in assessing risk posed by humans in a cyber network, and links human factor metrics to Hofstede's cultural dimensions [Hofstede 2011]. Issues related to insider threats and the factors leading to attacks where insiders are involved have been studied in [Colwill et al 2009]. It briefly discusses organisational and regional culture that affect insider threat metric.

Although human factors and the inclusion of cultural factors when studying humans have been discussed in detail in existing literature, we have not come across a parameterization method that leads to a holistic cybersecurity model, that incorporates humans and cultural factors along with technical metrics which are crucial to assessing cyber risk in a network. Thus, it is important to include humans and cultural factors as integral risk altering metrics in cybersecurity risk assessment models. Second, we present the development of a structure for the risk assessment process (Holistic Cybersecurity Risk Assessment Framework) and a framework for the execution of a risk assessment through risk parameterization (Multi-Level Risk Assessment Parameterization Framework). Third, we highlight a proof of concept application of the parameterization framework and the inclusion of human and cultural factors in risk models, using a malicious request to database server scenario. Fourth, we briefly discuss the inclusion of human factors and application of the presented frameworks to other instantiations of cybersecurity networks. Lastly, we address opportunities to apply these framework to future cybersecurity research.

Humans as Cybersecurity Risk Factors

Humans play a key role in cyber security applications because of their constant interaction with systems of high importance. Human factors in cyber security are generally explained by characterizing behavior of users, attackers and defenders, and how they contribute in introducing and mitigating risk in cyber systems. [Oltramari, et al, 2015] presents a human factors ontology, suggesting that trust placed in individuals is a pivotal element affecting their role within a cyber system. It suggests a framework to explore users, attackers and defenders based on their situational characteristics, behavioral characteristics, and knowledge and skill characteristics. Reliability on behavioral science theories to characterize human in cyber security scenarios, and empirical evaluation of their findings has also been discussed in [Pfleeger, Shari Lawrence, et al., June 2012].

Another important paradigm in defining human factors is the cultural factors, which greatly affect the structural, behavioral, and situational characteristics of humans. Adversaries with different cultural backgrounds are more likely to have a different course of action to reach a common end goal. [Henshel, D, et al, 2016 (cultural factors)) suggests that a single culture assumption for all attackers would not produce an accurate characterization of attackers. Attackers with the same end goals might have a different motivation. These methods form basis for our understanding of human characteristics and deciding the factors which have the most effect on the state of cyber security.

Integrating Human Factors in Cybersecurity Risk Modeling

Include references that help identify human characteristics which can be empirically studied and feasibly included in cybersecurity models.

The Use of Bayesian Network in Modeling of Complex Systems

Standard statistical techniques such as regression analysis are not suitable for risk assessment problems because they do not have any explanatory power. Risk assessment requires establishment of causal relationships between objective factors, which require a better modeling techniques than regression. The basic idea of regression analysis is to provide predictions of a certain event, given the evidence for correlated events, and it does a good job in a number of scenarios. Although, to use such a technique for evaluating causal relationships between risk factors can prove to be fatal, because the basic requirement of risk assessment is to be able to establish the factors which can be altered, so as to lower the risk in the system. [Fenton Norman, et al, CRC Press pg 31-33]

Moreover, cybersecurity risk modeling poses another challenge because it involves modeling complex systems and the interdependencies between its various components. Even understanding such systems can be a task, if components and their interdependencies are not appropriately visualized. Bayesian networks have proven to be efficient in modeling risk for such systems, since it allows visualizing various components in such systems as nodes, and their interdependencies as directed edges between nodes.

Bayesian networks provide a solution for studying classical cause-and-effect relationships. Since it combines graphical analysis with Bayesian analysis, it provides a more intuitive way to represent causal relationships. Bayesian networks are widely used to construct risk models to solve complex risk assessment problems *[Fenton Using Ranked Nodes to…]*. A simple Bayesian network is a directed acyclic graph where nodes are connected to represent conditional dependencies. For example - A node ‘X’ points

to node ‘Y’ when the probability distribution of Y is conditionally dependent on X; and possibly on other nodes too. The nodes in a Bayesian network can be thought of as random variables which could be discrete or continuous, and the edges as direct influence of a node on another. Root nodes in a Bayesian network are independent of any influence from any other components in the model, and each state has an associated probability that can be inferred from prior evidence. Each node in the network (which is not a root node) has a conditional probability table associated with it, which is defined by the probability of each of its state, given the evidence for its parents. Conditional probabilities can be inferred with observed data. At any instance, the probability distribution of a node is given by the observed value of some of its parents and the prior knowledge of the others . The probability distribution of root nodes are defined by the prior knowledge available for the occurrence of each of its state *[Weber- Overview on Bayesian Networks]*.

Owing to these properties, Bayesian networks provide an uncomplicated approach for analysing cybersecurity risk models. Especially, since our research aims to establish causal relationships between human factors and native components of a network, a graphical representation of dependencies is more intuitive and accessible.

3. Hypothesis

We hypothesize that risk in cyber systems can be dynamically assessed with each change in state of the system. To do so, we utilize the MulRAP Framework to choose risk metrics, and the Bayesian network to model their interactions and assess the variation in risk with change in state.

4. Methods

4.1 Parameter Selection: Using the MuLRAP framework to choose the risk parameters.

A hierarchical taxonomy of risk assessment parameterization is presented in this paper and organized into the Multi-Level Risk Assessment Parameterization Framework, which was developed through facilitated, collaborative, iterative, expert consultations with CyberSecurity Collaborative Research Alliance (CSec CRA) researchers over the course of a year. The participating CSec CRA researchers are experts in a wide variety of cybersecurity related fields including computer science, information security, computer engineering; software engineering; network science; intrusion detection; human-system integration, social and decision science, and risk assessment. Collectively, over the course of a year more than 30 CSec CRA researchers participated in weekly consultations to systematically conceptualize parameters (variables representing metrics) that could contribute to and/or mitigate risks of cybersecurity networks. The parameterization engendered the identification of multiple risk assessment taxonomy levels.
The first (top) risk assessment level specifies functional distinctions for system, asset, anti-asset, and policy. The system parameters incorporate the classic vulnerabilities, confidentiality, integrity, and accessibility/availability for the system of interest assessed at the system level (i.e. was the task completed without loss of message integrity, confidentiality, or functionality of the system), but also captures other mission-dependent vulnerabilities related to time, as timing can be a critical criterion for mission success.

The asset group captures hardware, software, and non-attacker human factors. The anti-asset group captures inherently malicious software and human factors (attackers). The policy group captures the design, implementation, compliance, and enforcement of organizational policies for human factor use of the system.

For each functional component (system, asset, anti-asset, and policy), the MulRAP framework follows the subsequent levels of the hierarchical taxonomy: risk assessment level (RAL), main assessment target (MAT), main assessment goal (MAG), assessment metric (AM), measurement metric (MM), and data uncertainty (DU; see Figure 5). The risk assessment sublevel is broken out into the components (physical and virtual) of the system being assessed. For example the "Asset" risk assessment level is comprised of the following risk assessment sublevels: hardware, software, the cloud, and the human components of a system (i.e. users, defenders, and attackers). The main assessment target identifies the specific component for which parameters and measurement metrics are being developed (i.e. the database server). The main assessment goal links back to the classic risk vulnerabilities quantified (or semi-quantified) in many risk assessment frameworks: Confidentiality, Integrity, and Accessibility. We add Time to this grouping as a main vulnerability as, for many cyber tasks, time windows (which can be process-limiting during the information flow for cyber processes and operation-limiting for the successful completion of a mission) are critical factors determining the success of the operation. Assessment metrics are the properties of the network for which one needs to quantify the risk [11]. These are usually the complex emergent properties, such as database information security. (The NIST cybersecurity framework calls these "metrics".) The measurement metrics (what NIST calls "measures") are quantifiable measures that (as best as possible) conform to the measurement metrics best practices (SMART: Specific, Measurable, Achievable, Realistic, Time-defined [12,13]. The uncertainty of each metric is characterized by its robustness, variability, and ultimately by its existence (not all identified measurement metrics are technically or logistically feasible). The characterization of, and explanation for, each taxonomic level is best illustrated through a tangible example.

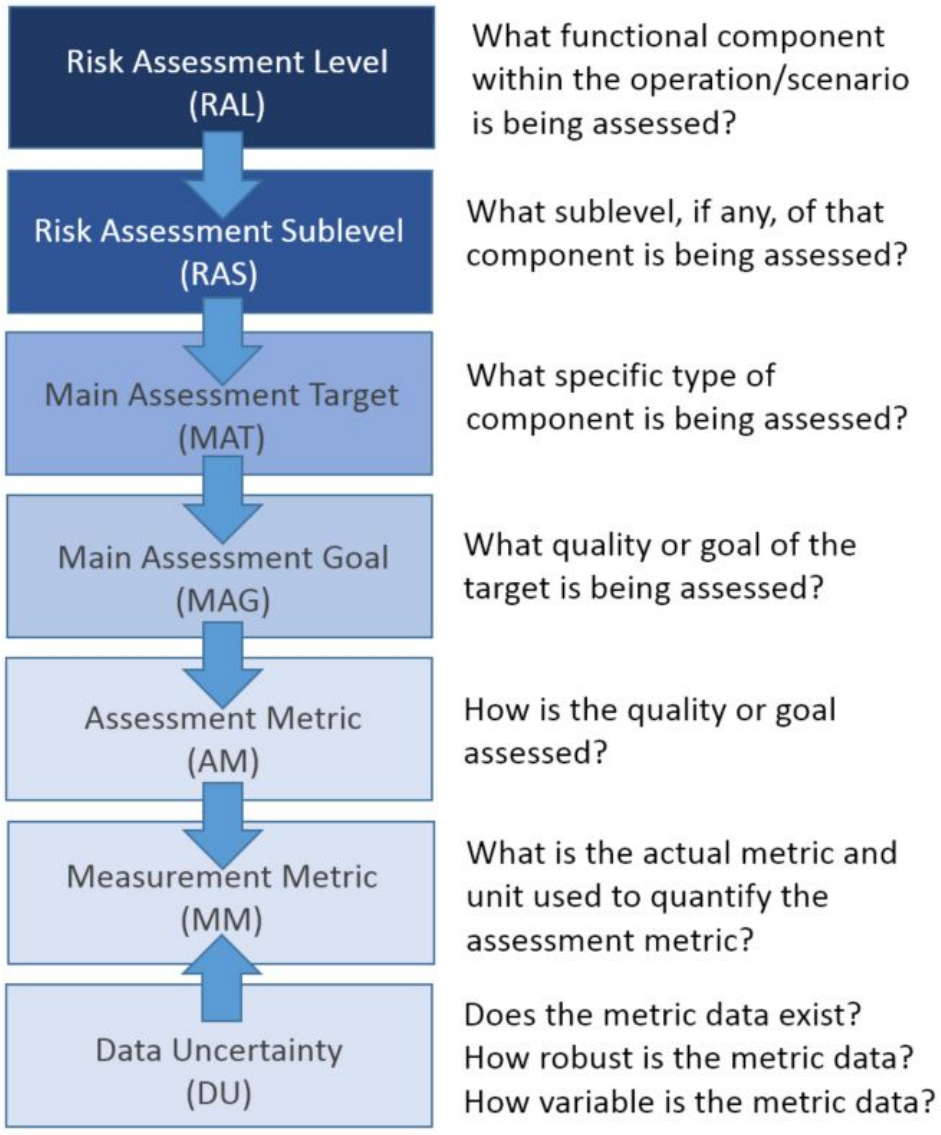


Figure x. Organizational levels of the risk assessment taxonomy within the Multi-Level Risk Assessment Parameterization Framework.

For example, the risk management question is to determine the vulnerability of a server to attacks via open server ports. To answer this risk management question, the risk assessor must know if the server has any open ports, the number of open ports, and the existence and type of port vulnerabilities. The first level of the hierarchical taxonomy (risk assessment level) asks what functional component within the operation/scenario is being assessed (e.g. system, policy, assets, and anti-assets)? The risk assessor must assess the assets of the network in the scenario. Second (risk assessment sublevel), what sublevel, if any, of that component is being assessed? An infrastructural/hardware asset is being assessed. Third (main assessment target), what specific type of component is being assessed? A server is being assessed. Fourth (main assessment goal), what quality or goal of the target is being assessed? The server's connection to the Internet is being assessed. Fifth (assessment metric), how is the quality or goal assessed? The presence of open ports while the server is connected to the internet will be assessed. Sixth (measurement metric),

what is the actual metric and unit used to quantify the assessment metric? The presence of open ports will be determined by the number of open ports on the server while connected to the Internet. Lastly, the seventh level of the hierarchical taxonomy addresses data uncertainty. Does the measurement data exist? Yes, it is possible to measure the number of open ports using readily available software tools. How robust is the measurement metric data? How reliable or variable is the measurement metric data? Measuring the number of open ports is a direct observation with no variability at any given point in time for the given server. However, if evaluated over the course of time, 95% confidence limits could be developed by averaging the data. Given that the open port data is readily available for servers, the risk assessor is able to quantify the number of open ports on the server and take the necessary actions to either close the open ports or further assess the vulnerability of the open ports. A visualization of this parameterization of open ports as a risk parameter for a server is illustrated in Figure y below. [Visualization of relevant parameterization needed]

Part 2. Parameters

The risk assessment taxonomic parameterization framework (i.e. MulRAP Framework) is applied by first identifying the complex system in question. The complex system is then deconstructed into its functional components and processes. The level of deconstruction is determined by the granular specificity of the risk assessment question. The functional components and processes (i.e. system/risk parameters) are then characterized based on the environmental context of the risk assessment question and the known vulnerabilities of the complex system in question. The relationship between the risk parameters representing the functional components and processes are then characterized based on available literature and empirical data. The risk model of the respective complex system is constructed using the risk parameters and relationships identified and characterized. The risk model is then validated via testbed implementation. The validation process and statistical analysis allows for the risk model to be modified in order to represent the minimum number of information-rich risk parameters that capture the risk of a system throughout an operation.

The parameterization of a complex system allows for risk assessors to choose risk metrics that will represent and model a given scenario. The risk metrics are chosen from the universe of risk metrics in the relevant taxonomies as determined by the risk parameterization effort. This parameterization method can be used for any scenario with a defined risk management question. The top down approach of system deconstruction followed by risk parameters and relationships identification and then risk model construction, identifies risk parameters for each assessment goal which then provides for the identification of quantifiable measurement metrics to quantify risk. Expert elicitation is then used to select the relevant assessment and measurement metrics from the universe of risk metrics (as determined by the risk parameterization effort).

To demonstrate the utility of this approach, we applied this risk assessment taxonomy and framework to an SQL database server inject scenario with the following as the guiding risk assessment question: “What is the associated risk, if an incoming connection to the database is successful?” In other words, we are quantifying the risk to the secure information in the database.

The risk assessment taxonomy and framework application is as follows:

- Risk Assessment Level: Database accessibility
- Risk Assessment Sublevel: Identification of which step in the access pathway is being modeled
- Main Assessment Target: The risk state after accepting connection request to the database
- Main Assessment Goal: Minimize risk (i.e. risk = low)
- Assessment Metric: Risk to the information in the database
- Measurement Metric: Risk Parameters
    - Port (P), Attacker Skill Indicator (AS), Connection (C0), Malicious IP Database (IP), Country Threat Index (CTI), Defense (D), User Permission (UP), Required Database Permissions (RDP)
- Data Uncertainty: Semi-quantitative metrics exist, variable robustness depending on risk parameters (e.g. provenance risk is well-documented in the literature, however provenance can be spoofed), for many risk parameters there are limited empirical (measured or experimental) data available.

Risk Parameters and **Computation Nodes**:

- Port (P)
- Attacker Skill Indicator (AS)
- Connection (C0)
- Malicious IP Database (IP)
- Country
    - Total # of Attacks
    - Malicious Saturation of Traffic
    - Hierarchical organization of attacker
    - Type of Attack
- **Weighted type of activity from country**
- **Country Threat Index (CTI)**
- **Connection Risk Prior to Defense**
- Defense (D)
- **Connection Risk After Defense**
- User Permission (UP)
- Required Access Level (AL)
- **Potential Access**
- **Risk to Database Compromise**

Figure : Conceptual Risk Framework

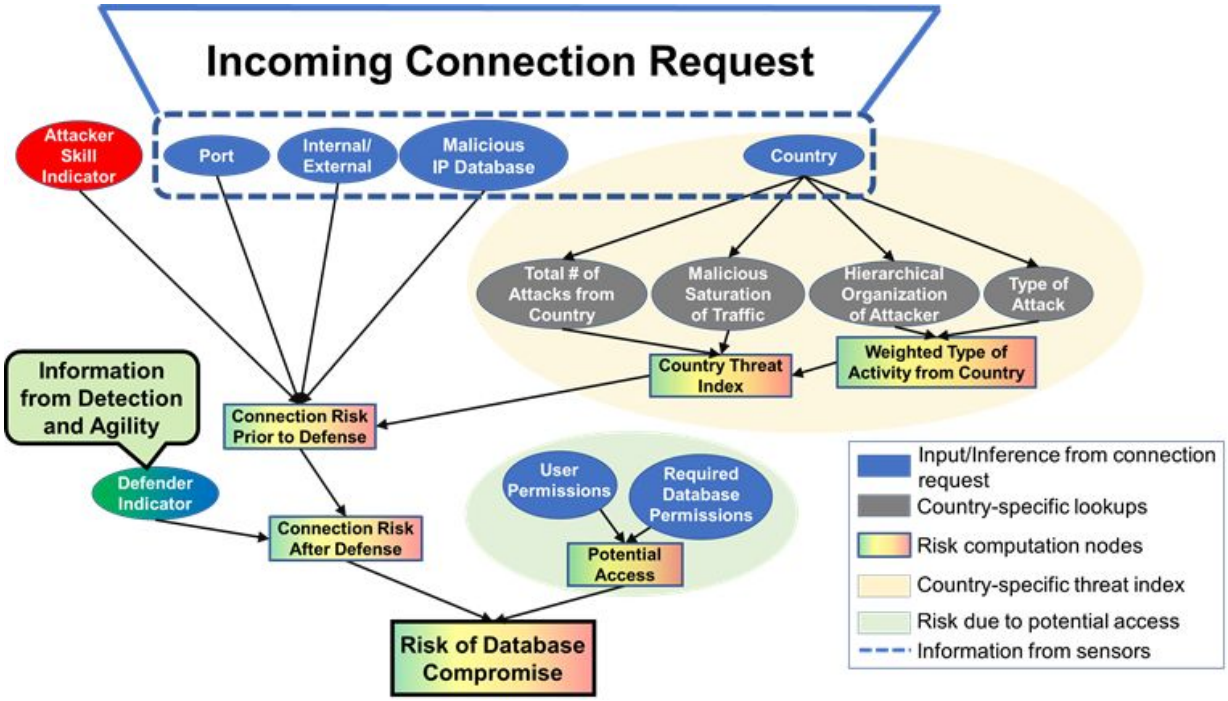


Table X. Description of clusters and their component risk metrics from Figure X.

Parameter Cluster	Description	Risk Metrics	Sources of Uncertainty
Connection Metrics	Metrics coupled with a connection request. IP address determines country.	Port; Internal/External; Online Malicious IP Database; Country	Skilled attackers can spoof IP address and appear to be on the internal network
Country-specific Metrics	Online lookup of statistical values specific to a country	Total # of Attacks; Malicious Saturation of Traffic; Hierarchical organization of attacker; Type of Attack	Not always feasible to trace the first true origin of the connection request
Attacker Skill Indicator	Attack frequency indicates attacker skill	Attacker Skill Indicator	Unlikely to identify Attacker Frequency during DDOS attacks
Defender Skill	Defender skill distribution estimated for model. Future potential for incorporating in real networks.	Defense	Variability due to physiological factors

Potential for database access	Aggregate and match of user permissions and required permission level for database access.	User Permission; Required Database Permission	Spoofing user permissions presents risk to the database
Risk of Database Compromise	Aggregated computation of risk to database	Risk of Database compromise	Model specification bias

The calculated database accessibility risk is a function of the above listed risk parameters (i.e. measurement metrics). High, medium, and low risk values were assigned to each risk parameter using literature based probabilities or reasonable estimates when no literature values were readily obtained. The joint probabilities of the risk parameters were calculated using a Bayesian approach for overall low-medium risk conditions (e.g. US-based provenance) and medium-high risk conditions (e.g. China-based provenance). The risk assessment taxonomy and framework for the database server proof of concept is laid out more completely in Henshel et al. [14].

Part 3. Relationships between parameters

It elaborates on how conditionality between risk metrics can be ascertained through intuition and logical reasoning.

Part 4. Risk computation nodes

A striking advantage of modeling cybersecurity risk using Bayesian networks over most statistical techniques is that it allows us to identify the factors which contribute the most towards high risk situations. The model we have built computes the risk due to a wide range of factors, from human factors such as defender and attacker skill to technical factors such as user permission and required access. Since these factors appear in clusters in our model, risk computation nodes have been introduced to aggregate risk due to the different cluster of factors in the model. For example, Country Threat Index node aggregates risk introduced due to country related factors, such as Hierarchical Organization of Attackers and Type of Attack by country. Having these nodes gives a better aggregation level for identifying factors that contribute the most to high risk situations.

The risk computation nodes that are used in our model are:

Weighted type of activity from country - Aggregates risk due to the type of activities and hierarchical organization of attackers that are prominent in a specific country

Country Threat Index - Aggregates and measures risk due to country-specific metrics

Connection Risk Prior to Defense - Aggregates risk from the connection metrics, before defender skill metric is accounted for

Connnection Risk After Defense - Aggregates risk after accounting for defender skill metric

Potential Access - What is the potential that the query is successful?

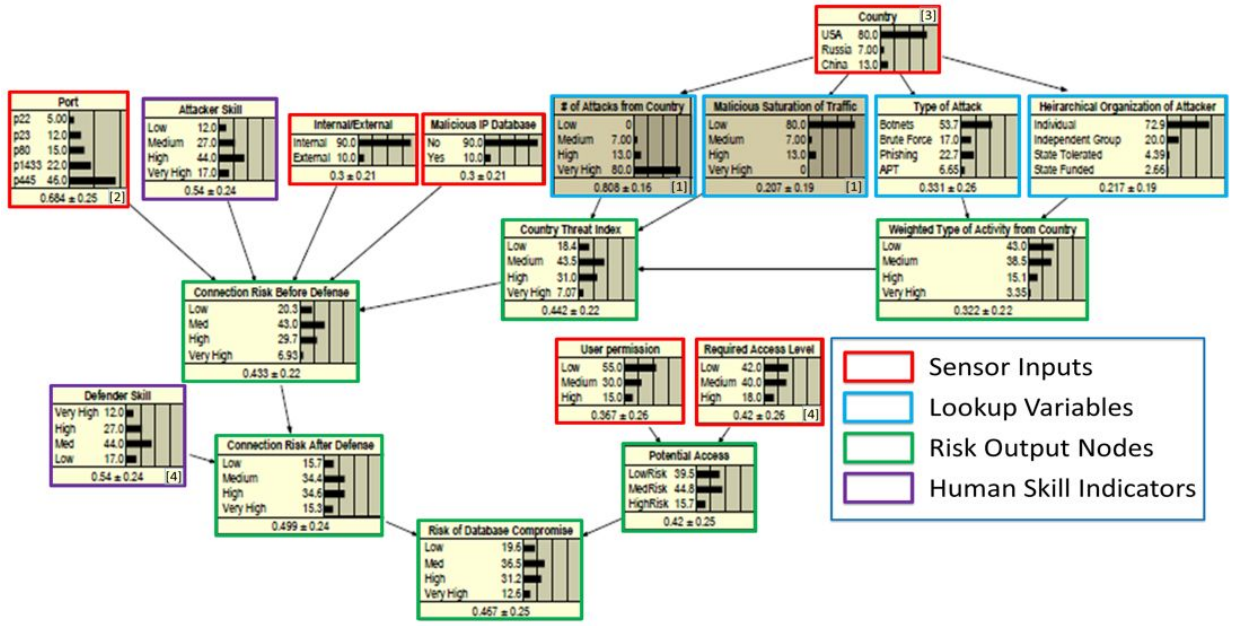
Risk of Database Compromise - Aggregate risk due to all the accounted metrics in final risk node

Part 5. Statistical Application

The interdependencies between the identified risk parameters and computation nodes are modeled using hybrid Bayesian networks over Netica by aggregating views and opinions of cybersecurity analysis, risk analysts, environmental scientists and data scientists. Each of the directed edges in Figure BN1 represent dependencies between risk metrics. Each node in the figure shows the marginal distribution for the node. The prior probabilities for sensor inputs and human skill indicators have been inducted from cyber reports. For example, prior distribution for Port is inducted from ports associated with most amount of attacks, as mentioned in Akamai Study 2011 Quarter 4 (insert ref). Defender skill metric is adapted from multiple questions in the Ponemon Study (insert ref) such as the defenders' familiarity with bypass techniques used by cyber criminals. Conditional probability tables are calculated by collaborating with experts in risk and cybersecurity.

In our final model, the risk to the database is calculated by the conditional probability P(R|S), which is the probability distribution of the risk to the database server, given the input state of the model S. The input state of the model is obtained by setting evidence for sensor inputs and human skill indicators.

Figure BN1 : Bayesian network implementation of the conceptual framework



5. Results

We present two scenarios to show the preliminary results obtained using our model. The first scenario, given the input state S1, is representative of low-medium risk to database. In contrast, the second scenario is representative of high risk to the database, given the input state S2. Input state S1 is set with evidence representative of lower risk scenarios, and S2 is set with evidence representative of higher risk scenarios. The statistical result in **Table R** shows that the model seems to be predicting risk distribution as expected.

Risk of database compromise, given S1, is skewed towards low to medium risk, and towards high risk given S2.

Table R: Results

Variable	State S_1	State S_2
Port (P)	p80 (Medium risk)	p22 (Very high risk)
Attacker Skill (AS)	Medium Skill (Medium to high risk)	Medium Skill (Medium to high risk)
Connection (C0)	Internal, (Low risk)	External, (High risk)
Malicious IP Database (IP)	Not listed, (Low risk)	Malicious Listed IP, (High risk)
Country Threat Index (CTI)	P(L| Country = USA) = 0.203 P(M| Country = USA) = 0.457 P(H| Country = USA) = 0.289 P(VH| Country = USA) = 0.051	P(L| Country = China) = 0.061 P(M| Country = China) = 0.308 P(H| Country = China) = 0.445 P(VH| Country = China) = 0.185
Defense (D)	High Skill (Medium to low risk)	High Skill (Medium to low risk)
User Permission (UP)	Low, (Low risk)	High, (High risk)
Required Access Level (RAL)	Low, (Low risk)	High, (High risk)
Risk of Database Compromise (R)	**$P(\text{Low Risk}\|S_1) = 0.383$** **$P(\text{Medium Risk}\|S_1) = 0.376$** **$P(\text{High Risk}\|S_1) = 0.161$** **$P(\text{Very High}\|S_1) = 0.08$**	**$P(\text{Low Risk}\|S_2) = 0.098$** **$P(\text{Medium Risk}\|S_2) = 0.215$** **$P(\text{High Risk}\|S_2) = 0.508$** **$P(\text{Very High Risk}\|S_2) = 0.179$**

6. Discussion

We present a systematic process for quantifying risk for cyber networks based on an iterative assessment process, much like the OODA loop [6] or the NIST cybersecurity framework process [5], and modeled after the 1997 Environmental Risk Assessment and Risk Management Framework [7]. Unlike the current and proposed NIST guidance, this process allows the risk assessor to identify quantifiable key risk parameters that can be used as measurement metrics within a risk equation. This process allows the risk assessor to develop value-based risk estimates at a level that is more precise than the non-quantified risk characterizations developed through the NIST process or the semi-quantitative high, medium, low risk estimates commonly used.

The MulRAP framework is a universal approach for parameterizing complex systems, facilitating the detailed characterization of the network structure and explications of the relationships between the nodes (components or assets) and edges (processes). The parameterization process can be applied to any high level concept (e.g. risk, vulnerability, resilience) quantitatively after defining, quantifying, and validating the relationships and inherent network properties. The goal of the parameterization process, as should be of any modeling endeavor, is to identify the minimum number of necessary and sufficient information-rich variables in order to accurately describe the emergent properties of a complex system.
(MISSING DISCUSSION OF RESULTS)

Discussion

Current Status of Cyberspace and Cybersecurity

The present nature of cyberspace requires sophisticated technology to determine risk of cyber attacks for any organization. With the increasing vastness of the internet, comes the need to develop risk frameworks which are responsive to the ever-changing nature of the cyberspace. Cyber-criminals are constantly adapting to the advancements made in cyber security technologies, and previously sophisticated attacks have become common and widespread. Ransomware attacks have been evolving in their methodological exploitation of known and unknown vulnerabilities existing in present systems, and have been causing major damage to businesses and individuals around the globe. Even some of the major firms believed to be pioneering in cutting edge cyber security measures have been made victims of attacks, resulting in terabytes of confidential information being leaked. [Symantec Volume 22, Internet Security Threat Report] mentions that cyber attackers are shifting their focus from economic espionage to politically-motivated attacks. Smarter and sophisticated cyber security measures are of national importance, with the attackers reaching out to disrupt the global political architecture. This calls for risk frameworks which are dynamic in nature, which means that they evolve along with the complexity and advancements of a network. Cyber security risk models should be developed in such a manner, so as to be resistant to the changing nature of networks, skills of adversaries and defenders, and the social and cultural factors which revolve around cyber networks.

In this paper, we present a Multi-level Risk Assessment Parameterization (Mul-RAP) framework, which evolves over currently available risk modeling approaches such as the NIST framework. It formulates a logically intuitive approach to cyber security risk modeling which addresses the need of developing dynamically calculated risk models by posing questions that aid in identifying essential risk-altering parameters for an organization.

Conclusion / Future Work -

Currently, we are applying this framework to a network model where each node represents components of a network that provides network access to a database where the operational state of each node is characterized as a combination of asset functionality (e.g. full or partial function) and infection state (e.g. infected or not infected). In the experiment we vary the asset operational state and characteristics of the nodes, and apply these modeled or applied microscale results to a network model that incorporates humans in the network as an asset contributing or mitigating risk.
After characterizing smaller, less complex networks we are using the MulRAP framework to help us combine models and develop a single, holistic cybersecurity model for a complex network, incorporating both humans and infection spread.

Our long-term goal is to employ this framework to quantify risk of any instantiation of a cybersecurity network, although this process is also applicable to any complex system. Such a goal requires the development of sufficient information about the most statistically significant and informative parameters for each network so that the risks can be calculated dynamically. By feeding in information from Intrusion Detection Systems, the risks can be used to inform recommended automated responses (agility maneuvers). The resulting state changes are then incorporated into the next iteration of the risk

calculations. Thus, the use of the Holistic Cybersecurity Risk Assessment (HCRA) Process with the Multi-Level Risk Assessment Parameterization (MulRAP) Framework for cybersecurity risk assessment will allow semi-automation of dynamic cybersecurity assessment and protective actions and enable risk assessors and risk managers to focus on the problems of detecting and responding to advanced persistent threats.

ACKNOWLEDGMENTS

The authors thank the Cybersecurity Collaborative Research Alliance researchers that participated in the risk parameterization process: J. Abbott, A. Alexeev, B. Bennett, B. Bertenthal, T. Braun, N. Buchler, H. Cam, L.J. Camp, G. Deckard, B. Dhoshi, L. Flora, W. Glodek, B. Hoffman, T. Kelley, D. Kelly, A. Kott, K. Levitt, H. Marshall, L. Marvel, I. Neamtiu, P. McDaniel, A. Oltramari, P. Rajivan, B. Rivera, J. Rowe, Q. Sun, A. Swami, D. Taylor, R. Walls, and F. Wu.

The researchers are sponsored by the U.S. Army Research Laboratory (ARL) Cybersecurity Collaborative Research Alliance (CSec CRA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the ARL, Department of Defense, Indiana University or any official policies of any of these entities.

References (incomplete)

Boccara, Nino. (2010). Modeling complex systems. Springer Science & Business Media.

Boyd, J. 1987. A discourse on winning and losing. Maxwell Air Force Base, AL: Air University Library Document No. M-U 43947

Collwill et al 2009 Colwill, Carl, ISTR, 2009

Doran, T.G. 1981. There's a S.M.A.R.T. way to write management's goals and objectives. *Management Review: AMA FORUM.* 70 (11): 35-36.

Funke, Joachim. (1991) "Solving complex problems: Exploration and control of complex systems." Complex problem solving: Principles and mechanisms: 185-222.

Koithan, Mary, et al, (2012) "A complex systems science perspective for whole systems of complementary and alternative medicine research." Forschende Komplementärmedizin/Research in Complementary Medicine 19.Suppl. 1: 7-14.

Henshel, D., Cains, M., Hoffman, B., and Kelley, T.. (2015). Trust as a Human Factor in Holistic Cybersecurity Risk Assessment. *6th International Conference on Applied Human Factors and Ergonomics*. 1117–1124.

Henshel, D., Sample, C., Cains, M., and Hoffman, B. (2016a) Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. *Proceedings of the 7th International Conference on Applied Human Factors and Ergonomics*.
Henshel, D., Alexeev, A., Cains, M.G., Cam, H., Hoffman, B., Neamtiu, I., Rowe, J.. (2016b) Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification. *Proceedings of the 15th IEEE International Symposium on Technologies for Homeland Security*.
Hofstede 2011
McQueen et al 2006 M.A, Mc Queen, et al, Quantitative cyber risk reduction.., 2006
NIST 2012 "Guide for conducting risk assessments," NIST Special Publication 800-30 rev.1
NIST, 2017 "Framework for Improving Critical Infrastructure Cyber Security," ver 1.1, Jan 10
Oltramari, A., Henshel, D., Cains, M., Hoffman, B. (2015). Towards a Human Factors Ontology for Cybersecurity. *Proceedings of the Tenth Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS).* 26-33
Presidential U. S. Congressional Commission on Risk Assessment and Risk Management . 1997. "Framework for Environmental Health Risk Assessment Final Report Volume 1." U.S. Congress, Washington, DC.
Roy et al 2010 Roy, Arpan, et. al, attack countermeasure trees, 2010
Suter, G.W. II. 2007 *Ecological risk assessment*. CRC press, 2nd Edition.
Yemm, G.. 2013. Essential Guide to Leading Your Team: How to Set Goals, Measure Performance and Reward Talent. Pearson Education. pp. 37–39. ISBN 0273772449.

TABLES AND FIGURES

Figure x. Holistic Cybersecurity Risk Assessment Framework: Adaptation of 1996 Presidential/Congressional Commission's Risk Management Framework and OODA loop to enhance the NIST cybersecurity risk framework.

Such a cybersecurity framework needs to be predictive in order to provide the necessary protections to prevent what would otherwise be considered zero-day attacks. The framework needs to be holistic and consider human factors (end users, defenders, and attackers) as risk mitigators and risk inducers just as much as hardware and software are generally considered risk components [8,9,10].

The first step in developing such a risk assessment framework is strategically organizing the contextual components for which the risk assessment is being conducted. This contextual organization is categorized as the Identify in NIST, Observe in the OODA Loop, the Problem/Context in the FEHRM, and Problem Formulation (identify information) in the HCRA Framework. In order to accurately formulate the risk management question and identify the information needed to answer the risk management question, the universe of the complex system must first be defined using a hierarchical taxonomy of risk assessment goals and risk assessment parameters.