Journal of Information Security, 2020, 11, 121-137
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Reducing Threats by Using Bayesian Networks to Prioritize and Combine Defense in Depth Security Measures

Rodney Alexander

Hutchinson Community College, Hutchinson, Kansas, USA
Email: rdnyalex@aol.com

How to cite this paper: Alexander, R. (2020) Reducing Threats by Using Bayesian Networks to Prioritize and Combine Defense in Depth Security Measures. *Journal of Information Security*, **11**, 121-137.
https://doi.org/10.4236/jis.2020.113008

Received: April 28, 2020
Accepted: June 5, 2020
Published: June 8, 2020

Abstract

Studied in this article is whether the Bayesian Network Model (BNM) can be effectively applied to the prioritization of defense in-depth security tools and procedures and to the combining of those measures to reduce cyber threats. The methods used in this study consisted of scanning 24 peer reviewed Cybersecurity Articles from prominent Cybersecurity Journals using the Likert Scale Model for the article's list of defense in depth measures (tools and procedures) and the threats that those measures were designed to reduce. The defense in depth tools and procedures are then compared to see whether the Likert scale and the Bayesian Network Model could be effectively applied to prioritize and combine the measures to reduce cyber threats attacks against organizational and private computing systems. The findings of the research reject the H_0 null hypothesis that BNM does not affect the relationship between the prioritization and combining of 24 Cybersecurity Article's defense in depth tools and procedures (independent variables) and cyber threats (dependent variables).

Keywords

Information Assurance, Bayesian Networks, Influence Diagrams, Defense in Depth, Information Technology, Network Security, Cybersecurity

1. Introduction

Cyber-attacks can be reduced by deploying security tools and procedures. These systems of network defense methods are primarily comprised of static defenses focused on preventing attacks from entering a network by enabling the features of blocking access, requiring authentication, or analyzing traffic [1]. Defense in depth (DiD) prevents network intrusions by deploying tools and procedures such as firewalls, access control and detection.

The strategy recommends a balance between the protection capability and cost, performance, and operational considerations [2]. The entire business process is kept in focus when developing plans to deploy defense in depth. The probability that defense in depth measure can reduce cyber threats is quantifiable.

Bayesian networks are direct acyclic graphs in which the nodes represent propositions (or variables), the arcs signify the existence of direct casual dependencies between the linked propositions; the strengths of these dependencies are quantified by conditional probabilities [3].

Reducing security threats are dependent on the probability of being reduced by security tools and procedures. To adapt to the ever-changing threat profile of network attacks, the DiD model must be adapted to be symmetric and focus on new vectors for defense instead of authenticating, blocking, or analyzing all traffic [1].

New threats appear daily, security analysts can use defense in depth to prioritize defensive measures to face those threats. The Bayesian network theory can be deployed in the information assurance planning process. The logic of the theory can easily be extended to decisions about selecting goals or managerial strategy [4].

Organizations can develop plans to target certain threats with Bayesian reasoning.

Instead of a focusing on feature-centric network defense requirements, the defense in depth (DiD) model should be redesigned to be a functional or capability focused model [1]. Defense in depth priorities and focus should align with current threats, for example DDOS and DOS attacks. Bayesian network theory is often depicted using influence diagrams.

An influence diagram is a network representation for probabilistic and decision analysis models [5]. Information assurance decisions are graphically displayed using information assurance influence diagrams. Decision theory provides a normative framework for representing and reasoning about decision problems under uncertainty [6].

The ambiguity of deciding which defense in depth measures to use to reduce network intrusions can be solved using this modeling principle. Siymmetry in the DiD model allows for the network defense system to recognize the insider threat, preventing data exfiltration and allowing attacks to be stopped at the originating network instead of being defended by the attacked network [1]. Both internal and external audits are DiD measures when combined with encryption can help to prevent both inside and outside attacks.

The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods [7]. Defense in depth measures should be arrayed against threats to attack them from several different directions. Dynamic defenses must also be enabled, which change attack surfaces to proactively defend a network [1].

Defense in depth intrusion detection systems can adjust to the changing nature of attacks.

Individual defense in depth measures, for example firewalls have been proven to reduce cyber-attacks. At its core, Bayes's theorem depends upon an ingenious turnabout: If you want to assess the strength of your hypothesis given the evidence, you must also assess the strength of the evidence given your hypothesis [8]. The 24 Network security articles provide a strong signal that the premise of arraying certain network security measures against certain threats can be successful. In this study the decision to deploy a certain network security measure is displayed as a node.

The nodes correspond to variables which can be constants, uncertain quantities, decisions, or objectives [5]. The security tool and procedure variables represent decisions that information security professionals use to protect their networks. This research study explores whether the Bayesian Network Model (BNM) can be effectively applied to the array of information assurance defense in-depth measures to mitigate network security threats.

1.1. Cloud Security

Today, with the rise of managed security services and other outsourced network services, additional security can be provided inside the cloud [7]. Defense in depth can also be extended to protect resources in the cloud in Security as a Service. Traditionally, security was implemented at the endpoints, because that's what the user controlled [7].

Today it is important to deploy defense in depth measures and tools such as encryption and authentication to cloud resources. If we could build a new Internet today from scratch, we would embed a lot of security functionality in the cloud [7]. Today's deployment of defense in depth should include measures and tools which cover cloud resources.

Defense in depth beats a single point of failure, and security in the cloud is only part of a layered approach [7]. The layered defense in depth approach must also include cloud security features. Smart organizations build defense in depth: e-mail filtering inside the cloud plus anti-virus on the desktop [7].

The holistic approach to defense in depth must take resources from cloud to desktop into consideration. Security would be vastly improved if the major carriers implemented cloud-based solutions, but they're no substitute for traditional firewalls, IDSs, and IPSs [7]. Although an organization's resources are in the cloud, traditional defense in depth tools and measures are still applicable.

This should not be an either/or decision [7]. Security is about technology, people, and processes [7]. The entire organizational digital umbrella falls in the realm of defense in depth.

One of the basic philosophies of security is defense in depth: overlapping systems designed to provide security even if one of them fails [7].

With a defense in depth approach, the network remains secure even if one of the network tools fail, another tool or procedure should be designed to step in and take the place of the failed tool. An example is a firewall coupled with an intrusion-detection system (IDS) [7]. The network remains secure by using with two security tools working together.

Defense in depth provides security, because there's no single point of failure and no assumed single vector for attacks [7]. Networks today require constant connectivity. Defense in depth helps to provide constant connectivity with redundant security measures and tools.

1.2. Control System Security

As in common networking environments, control system domains are subject to myriad vulnerabilities and holes that can provide an attacker a "backdoor" to gain unauthorized access [9]. Network intrusions are commonplace on control systems partly due to network vulnerabilities. Given the reliance of control systems on the storage, accuracy, and accessibility of command and control data, as well as the prevalence of system query language (SQL) databases on these types of networks, standard SQL injection techniques against control system components pose a major threat to control system security [9].

Control system security plays a major role in the national infrastructure security system.

What makes this interesting, and also a concern, is that the traditional mitigation strategies for common networks are not always effective or practical in control systems architectures [9]. New concepts for managing control system security must be developed.

Applying security patches to operating systems and applications that run control systems is not a trivial endeavor [9]. Traditional software patch management systems were not developed for control systems. Prior to modification, rigorous testing must be completed to ensure that modifications do not impact operations [9].

Control systems cannot afford to be interruptions due to faulty software patch installations. By gaining access into a field device, the attacker can become part of the sensor network and "tunnel" back into the control system network [9]. Control systems require end to end security.

If a device is compromised, and the attacker can leverage control over the device and escalate privileges, the attacker can begin to execute several procedures, including scanning back into the internal control network, altering the data that will be sent to the control master, or changing the behavior of the device itself [9]. Strict procedures and security tools must be deployed on control systems to limit what device can and cannot do. Database applications have become core application components of control systems and their associated record keeping utilities [9].

Pen testing and IDS systems are just a few security procedures and tools necessary to keep control systems secure. Control system environments have traditionally been (or been intended to be) protected from non-authorized persons by air gapping [9]. Today air gapping as a form of security for control systems is unpractical because most systems are tied to the Internet or as a minimum the organizations intranet.

Three of the key security issues that arise from assumed trust are 1) the ability for an attacker to re-route data that is in transit on a network, 2) the ability to capture and analyze critical traffic that is in plaintext format, and 3) the ability to reverse engineer any unique protocols to gain command over control communications [9]. Control systems should be protected from Man in the Middle attacks and intrusions by using encryption and intrusion detection systems.

2. Theoretical/Conceptual Framework

2.1. Bayesian Networks

Specifically Bayes's theorem states that the posterior probability of a hypothesis is equal to the product of (a) the prior probability of the hypothesis and (b) the conditional probability of the evidence given the hypothesis, divided by (c) the probability of the new evidence [8].

The reduced threat is equal to the network security measure plus the network security procedure divided by each or two $P = (N + N)/2$.

Bayes's theorem, named after the 18th-century Presbyterian minister Thomas Bayes, addresses this selfsame essential task: How should we modify our beliefs in the light of additional information [8]? Network security confidence can be enhanced by the theory of linking network security tools and procedures to network threats. Bayesian decision theory was used because its principles can be applied as a systematic approach to complex decision making under conditions of imperfect knowledge [10].

Information assurance decision making can be improved by using an organized Bayesian approach. This research provides a systematic approach to reduce cyber threats, which may be of interest to the scholar-practitioner community. After actively collecting or happening upon some potentially relevant evidence, we use Bayes's theorem to recalculate the probability of the hypothesis in light of the new evidence.

After combining the measures and tools, their ability to reduce security threats was recalibrated [8]. This revised probability is called the posterior probability or simply the posterior. The arcs reveal the probabilistic dependence of the uncertain quantities and the information available at the time of the decisions [5].

This revised probability is called the posterior probability or simply the posterior.

The revised post experimental probability that the combining (arraying) of security procedures and measures can help reduce network threats is outlined in the experiment's conclusions.

A network of this sort can be used to represent the deep casual knowledge of an agent or a domain expert and turns it into a computational architecture if the links are used not merely for storing factual knowledge but also if directing and activating the data flow in the computations which manipulate this knowledge [3].

By using Bayesian networks, the experience of security analysis is actively applied to threat reduction instead of being stored in a static location. In the face of uncertainty, a Bayesian asks three questions: How confident am I in the truth of my initial belief [8]? It is a fair assumption that a systematic approach should be taken in the deployment of information assurance measures.

We then quote results which show that these objectives can be fully realized only in singly connected networks, where there exists only one (undirected) path between any pair of nodes [3]. The relationship to combined security tool and procedure variables are singularly connected to reduced security threat nodes. It is an intuitive framework in which to formulate problems as perceived by decision makers and to incorporate the knowledge of experts [11].

Influence diagrams display how Trojan Horses are reduced by combining antivirus tools with applying security patches procedures as outlined by security professionals. Security tools and procedures from 24 information security articles are prioritized using the Likert Scale (**Table 1**).

The Bayesian Network experimental model (influence diagrams) was used to depict the results of combining the defense in depth measures to reduce security threats. Influence diagrams show how dependencies and conditional-independence relationships can be tested in simple link-tracing operations [3]. Reduced security threats can be directly connected to combined threats and procedures.

On the assumption that my original belief is true, how confident am I that the new evidence is accurate [8]? The arraying of network security procedures and tools against certain threats by network security research, lends proof that the Bayesian systematic approach is a plausible solution. And whether or not my original belief is true, how confident am I that the new evidence is accurate [8]?

Using a Bayesian Network example (**Table 2**) we can show the accuracy of combining tools and procedures to reduce security threats.

2.2. Influence Diagrams

An influence diagram (ID) (also called a relevance diagram, decision diagram or a decision network) is a compact graphical and mathematical representation of a decision situation [12]. Deciding which defense in depth tools and procedures to combine to combat certain threats can be displayed in an influence diagram (**Figure 1**).

Decision node (corresponding to each decision to be made) is drawn as a rectangle [5].

The decision to combine a certain security tool and procedure represent a decision node.

An ID is a directed acyclic graph with three types (plus one subtype) of node and three types of arc (or arrow) between nodes [11]. The influence (arc) of security tools and procedures (decision nodes) on security threats (value nodes) can be displayed in the influence diagram.

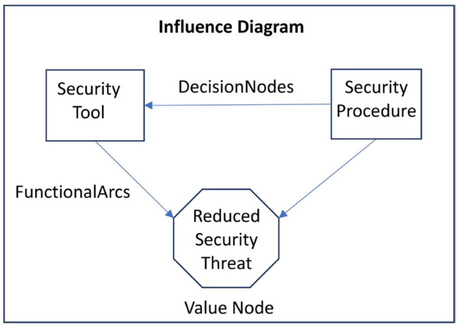

Figure 1. Influence diagram.

Table 1. Top ten security tools and procedures prioritization.

Priority	Tools	Procedures
1	Encryption	Require Authentication
2	Hash	Require Authentication
3	Anti-virus	Apply Patches
4	IDS	Conduct Pentest
5	Anti-virus	Conduct Pentest
6	Firewall	Conduct Pentest
7	Firewall	Create DMZ
8	One-time Token	Require Authentication
9	VPN	Conduct Internal Audit
10	PKI	Require Authentication

Table 2. Bayesian design model example.

		Bayesian Design Model Example			
		Mitigation Procedures			
		a (10)	**b (9)**	**c (8)**	**d (7)**
Mitigation Tools	**x (10)**	10 = (10 + 10)/2 *reduces threat g*	9.5 = (9 + 10)/2 *reduces threat j*	9 = (8 + 10)/2 *reduces threat m*	8.5 = (7 + 10)/2 *reduces threat p*
	y (9)	9.5 = (10 + 9)/2 *reduces threat h*	9 = (9 + 9)/2 *reduces threat k*	8.5 = (8 + 9)/2 *reduces threat n*	8 = (7 + 9)/2 *reduces threat q*
	z (8)	9 = (10 + 8)/2 *redcues Threat i*	8.5 = (9 + 8)/2 *reduces threat l*	8 = (8 + 8)/2 *reduces threat o*	7.5 = (7 + 8)/2 *reduces threat r*

Note: $p = (a + x)/2$

An influence diagram is a graphical structure for modeling uncertain variables and decisions and explicitly revealing probabilistic dependence and the flow of information [11]. Penetration testing (pen testing) and IDS are combined to influence the reduction of DOS and DDOS attacks as displayed in the below influence diagram. Value node (corresponding to each component of additively separable Von Neumann-Morgenstern utility function) is drawn as an octagon (or diamond) [5].

Reduced security threats for example distributed denial of service (DDOS) and man in the middle (MitM) attacks are represented as value node variables. It is a generalization of a Bayesian network, in which not only probabilistic inference problems but also decision-making problems (following the maximum expected utility criterion) can be modeled and solved [12]. Network security issues can be displayed and resolved using the Bayesian network design model.

Since the diagram can be analyzed directly, there is no need to construct other representations such as a decision tree [11]. Expedient results to reducing network threats are easily displayed using influence diagrams. Decision nodes and incoming information arcs collectively state the alternatives (what can be done when the outcome of certain decisions and/or uncertainties are known beforehand) [5].

The outcomes of combining security tools and procedures are shown in decision nodes and function arcs. An influence diagram is a theoretically based aid for obtaining the decision-makers structure for a complex decision problem under uncertainty [12]. Information security managers can clear up some of the ambiguity of information assurance by using influence diagrams.

Value nodes and incoming functional arcs collectively quantify the preference (how things are preferred over one another) [5]. The partiality of combining the tool and procedure variables is clearly shown in the value and incoming functional arcs. Bayesian probability is an interpretation of the concept of probability, in which, instead of frequency or propensity of some phenomenon, probability is interpreted as reasonable expectation [13] representing a state of knowledge [14] or as quantification of a personal belief [15].

Based on the information gained in this experiment it is believed that the combining of security procedures with security tools is an effect and systematic way to reduce security threats.

Professor Ronald Howard from Stanford University and his colleague, Dr. James Matheson, refined and popularized influence diagrams as a convenient notation for communicating about decision problems, that is complementary to decision trees [16]. The daunting task of how to constantly combat security threats can be effectively discussed using influence diagrams.

Advantages of using an influence diagram are rapid identification of important state and decision variables, a more balanced decision model, and the direct construction of the decision tree [12]. Using influence diagrams, the proper security tools and procedures can be quickly identified to combat specific security threats. I have attempted to extend the notion of an influence diagram so that it can be used by the decision analyst to conceptualize the relationship between the probability distributions on different variables ln a decision model [12].

Decision-makers can easily visualize using influence diagrams (Table 3) how threats are reduced by combining the relationship of security measures and procedures.

Table 3. Influence diagram table.

Mitigation Procedures								
Mitigation Tools	**1) Require Authentication**	**2) Apply Patches**	**3) Create DMZ**	**4) Conduct Internal Audit**	**5) Conduct PEN Testing**	**6) Require Employee Training**	**7) Social engineering testing**	**8) Conduct External audit**
1) Encryption	10 Virus, Intrusion, Data & Privacy Loss, DDOS, MitM	1 Intrusion		1 Insider	1 Privacy Loss	1 ID Theft		1 Customer Data Loss
2) Hash	5 Privacy, Data Loss, Password Cracking, Sabotage							
3) Anti-virus	2 Virus	4 Trojan, Virus		1.5 Malware, Data Loss	3 Adware, DDOS, Intrusion			
4) IDS		2 Virus, DOS	2 Intrusion, Zero Day		3.5 DOS, DDOS		1 Ransomware	2 Data Loss, DDOS
5) Access control lists	3 DOS, Data Loss	2 Intrusion, DOS	1 Spyware					
6) Firewall			2 Zero Day, DNS Attack		2 Intrusion, DDOS	1 Watering-Hole		
7) One-time tokens	2 Virus, Data Loss							
8) VPN								2 Data Loss, MitM
9) PKI	2 MitM, DDOS							2 Data Loss
10) Anti-spyware	1 Spyware	1 Spyware			1 DDOS	1 Phishing	1 Spyware	
11) Biometrics						1 Password Sniffing	1 Password Sniffing	
12) Vulnerability tools		1 Zero Day		1 Data Loss	1 Intrusion			

Note: $p = (a + x)/2$

The analysis can be performed using the decision maker's perspective on the problem [11]. The network security problem can then be seen from the security manager's point of view.

An influence between two random variables, x and y, ls said to exist when the variables are not probabilistically independent [12]. Network security tools and procedures are variables that can work together to decrease threats against the network. Modifications to the model suggested by such analyses can be made directly to the problem formulation, and then evaluated directly [11].

Security analyst can provide feedback on how the tools and procedures are arrayed against the threats. Each influence diagram is an assertion of probabilistic dependence [12].

This study shows using influence diagrams, that there is a combined relationship between security tools and measures variables and an inverse relationship with the variable—security threat.

3. Methodology

3.1. Research Design

This experimental survey research design was used to survey a simple random sample frame of 24 peer reviewed information security research articles. The peer reviewed information security research articles were scanned for a list of ten network security tools and procedures.

The prioritization was done using a Likert scale instrument with a (1-10) prioritization of the tools and procedures listed most frequently in the peer reviewed articles.

3.2. Data Analysis

The data analysis was conducted using a Likert Scale, with a (1-10) prioritization of 10 network security tools and procedures and the BNM to conduct a pair-wise comparison of each of the ten tools and procedures to their ability to reduce threats to network security. The research methods used in the study provided the advantage of using statistics to make inferences about larger groups, using very small samples, referred to as generalizability [17]. The findings are presented in the results section.

4. Results

The purpose of this chapter is to present the analysis which reject the H_0 null hypothesis that BNM does not affect the relationship between the prioritization and combining of 24 Cybersecurity Article's defense in depth tools and procedures (independent variables) and cyber threats (dependent variables). Beginning with a provisional hypothesis about the world (there are, of course, no other kinds), we assign to it an initial probability called the prior probability or simply the prior [8]. Data collected before the analysis in this experiment shows a lack of combining security measures and tools to combat specific security threats.

The data capture (recording) and coding methodology employed in this study was used to determine the best defense in-depth choices from a list of decision alternatives (network security threats). Finally, a summary of the results is included in this chapter.

5. Investigative Questions

The study design included one investigative question which provided foundation for the main research questions. This section lists the investigative question and includes the statistical analysis to explore the question.

Investigative Question 1

Of the ten network security tools and procedures, prioritize them according to their prioritization from 24 Network Security Articles. A Bayesian Network model was then used to array network threats to defense in depth measures. An influence diagram is an intuitive visual display of a decision problem [16].

Network security issues for example, viruses, spam and phishing attacks can be graphically displayed using influence diagrams. It depicts the key elements, including decisions, uncertainties, and objectives as nodes of various shapes and colors. It shows influences among them as arrows [16]. The effects of using security tools such as antivirus and procedures such as pen testing can be shown using shapes colors and arrows.

6. Discussion

The current agenda of prioritizing and combining defense in depth measures can continue to evolve based on this investigation. New vectors, such as dynamic network addressing, enterprise computing resources, and network architectures, must be used by the DiD model to prevent attacks from reaching network, consuming attackers often limited resources, and securing networks in their design and architecture [1]. Defense in depth takes a holistic approach to network security, protecting the network from several different perspectives with both tools and procedures.

We found that when a decision maker identified the existence of an influence, the variables later turned out to be probabilistically dependent [12]. The reduction on network security threats can be influenced by the combination of security measures and tools. Encryption and requiring authentication were listed as most the most effective tools and procedures when dealing with threats such as viruses, data/privacy loss and Man in the Middle attacks. Additionally, using hash algorithms and requiring authentication was can be used to stop password cracking and sabotage.

7. Conclusions

The research concluded that the Bayesian Network Model process can play a role in the organization's decision process to arraying and combining defense in depth measures against network threats. In a scenario where an attacker is actively attempting to gain access from the internet, a defense in depth strategy will deflect the attack, assuming that security measures like Network Address Translation (NAT), a firewall, a Demilitarized Zone (DMZ), and gateway Intrusion Detection System (IDS) are in place [2]. A combination of both security procedures and security tools plays an important role in defense in depth.

Large infrastructures must be protected against sophisticated attacks on organizational, technical and logical levels [18]. Advanced Persistent Threats (APT) which target many large organizations; can only be stopped with a layered defense approach. A secure computing system is provided which utilizes a unique combination of Public Key Infrastructure (PKI), Virtual Private Networking (VPN), and server-based computing on thin client devices [19].

Defense in depth tools and procedures are combined to create a secure computing environment. Defense in depth concept has emerged as a model to isolate key resources with protective layers [20]. A layered security blanket can be placed around critical information infrastructure to protect them from cyber criminals.

The available published knowledge of BNM can be used to prioritize defense in depth measures against network threats. This is confirmed by the research conclusion. Defense in depth decision making can be deployed using BNM to enhance organizational IT security. Defense in depth and BNM can be an important asset to the organization. Further advances can be gained in the use of defense in depth by continuing BNM.

To better understand the role that BNM can play in IT security, this research proposed a BNM structural and measurement model of the relevant factors. The future of IT security should include additional exploratory models to advance understanding of why the current models are not substantially improving IT security. To understand the shortcoming of current IT security models, further exploratory studies should be conducted on additional models.

Ethical Considerations

The potential benefits of research in organizations, especially public safety organizations, can be very beneficial, but there are risks that some employees or the organization could be unfairly stigmatized. This study was conducted with the informed consent of all the participants. The participants were not subjected to risk. To avoid conflict of interest, the survey participants are in no way related to the researcher.

Consent for Publication

For specifically addressing autonomous agency, the design included an informed consent process to ensure that participation was voluntary, with adequate information provided to participants to make their decision of whether or not to participate [21]. Specifically addressing diminished autonomy, while ensuring extra protection is afforded to prevent harm from exclusion.

Availability of Data and Material

All datasets on which the conclusions of the manuscript rely will be deposited in publicly available repositories (where available and appropriate) supporting files, in machine-readable format (such as spreadsheets rather than PDFs).

Funding

There was no outside funding for this article.

Authors' Contributions

Rodney Alexander is the sole author of this article.

Acknowledgements

Capella University Dissertation Committee.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Groat, S., Tront, J. and Marchany, R. (2012) Advancing the Defense in Depth Model. 7*th IEEE International Conference on System of Systems Engineering*, Genova, 16-19 July 2012, 285-290. https://doi.org/10.1109/SYSoSE.2012.6384127

[2] Cleghorn, L. (2013) Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *Journal of Information Security*, **4**, 144-149. https://doi.org/10.4236/jis.2013.43017

[3] Pearl, J. (1985) Bayesian Networks: A Model of Self-Activated Memory for Evidential Reasoning (UCLA Technical Report CSD-850017)*. Proceedings of the Seventh Annual Conference of the Cognitive Science Society*, Irvine, 15-17 April 1985, 329-334. http://ftp.cs.ucla.edu/tech-report/198_-reports/850017.pdf

[4] Meier, K.J., Favero, N. and Zhu, L. (2015) Performance Gaps and Managerial Decisions: A Bayesian Decision Theory of Managerial Action. *Journal of Public Administration Research and Theory*, **25**, 1221-1246. https://doi.org/10.1093/jopart/muu054

[5] Shachter, R.D. (1988) Probabilistic Inference and Influence Diagrams. *Operations Research*, **36**, 589-604. https://doi.org/10.1287/opre.36.4.589

[6] Haddawy, P. (1999) An Overview of Some Recent Developments in Bayesian Problem-Solving Techniques. *AI Magazine*, **20**, 11.

[7] Schneier, B. (2006) Security in the Cloud.

[8] Paulos, J.A. (2011) The Mathematics of Changing Your Mind [by Sharon Bertsch McGrayne]. Book Review. *New York Times*.

[9] Kuipers, D. and Fabro, M. (2006) Control Systems Cyber Security: Defense in Depth Strategies (No. INL/EXT-06-11478). Idaho National Laborat.

[10] Stankovic, J.A. (1985) An Application of Bayesian Decision Theory to Decentralized Control of Job Scheduling. *IEEE Transactions on Computers*, **34**, 117-130. https://doi.org/10.1109/TC.1985.1676548

[11] Shachter, R.D. (1986) Evaluating Influence Diagrams*. Operations Research*, **34**, 871-882. https://doi.org/10.1287/opre.34.6.871

[12] Howard, R.A. and Matheson, J.E. (1984) Influence Diagrams. In: Howard, R.A. and Matheson, J.E., Eds., *Readings on the Principles and Applications of Decision Analysis*, Vol. II, Strategic Decisions Group, Menlo Park.

[13] Cox, R.T. (1946) Probability, Frequency, and Reasonable Expectation. *American Journal of Physics*, **14**, 1-10. https://doi.org/10.1119/1.1990764

[14] Jaynes, E.T. (1986) Bayesian Methods: General Background. In: Justice, J.H., Ed., *Maximum-Entropy and Bayesian Methods in Applied Statistics*, Cambridge University Press, Cambridge, 1-25. https://doi.org/10.1017/CBO9780511569678.003

[15] de Finetti, B. (2017) Theory of Probability: A Critical Introductory Treatment. John Wiley & Sons Ltd., Chichester. https://doi.org/10.1002/9781119286387

[16] Influence Diagrams. http://www.lumina.com/technology/influence-diagrams

[17] Cooper, C.R. and Schindler, P.S. (2008) Business Research Methods. 10th Edition, McGraw-Hill, Boston.

[18] Balcerek, B., Frankowski, G., Kwiecień, A., Smutnicki, A. and Teodorczyk, M. (2012) Security Best Practices: Applying Defense-in-Depth Strategy to Protect the NGI_PL. In: *Building a National Distributed e-Infrastructure-PL-Grid*, Springer, Berlin, Heidelberg, 128-141. https://doi.org/10.1007/978-3-642-28267-6_10

[19] Neumann, W.C., Corby, T.E. and Epps, G.A. (2008) U.S. Patent No. 7,428,754. U.S. Patent and Trademark Office, Washington DC.

[20] Goztepe, K., Kilic, R. and Kayaalp, A. (2014) Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey. *Journal of Naval Science and Engineering*, **10**, 1-24.

[21] National Commission for the Protection of Human Subjects (1979) Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Department of Health and Welfare, Washington DC.

[22] Chen, P., Desmet, L. and Huygens, C. (2014) A Study on Advanced Persistent Threats. In: *IFIP International Conference on Communications and Multimedia Security*, Springer, Berlin, Heidelberg, 63-72. https://doi.org/10.1007/978-3-662-44885-4_5

[23] Dictionary, M.W. (2015) An Encyclopedia Britannica Company. http://www.merriam-webster.com/dictionary

[24] Singh, A. and Bora, M.S. (2013) Cyber Threats and Security for Wireless Devices. *JECET*, **2**, 277-284. https://doi.org/10.2139/ssrn.3419703

[25] Rouse, M. (2007) Defense in Depth. http://searchsecurity.techtarget.com/definition/defense-in-depth

[26] Cobb, M. (2014) Firewall. http://searchsecurity.techtarget.com/definition/firewall

[27] Cole, B. (2014) Intrusion Detection System. http://searchcompliance.techtarget.com/definition/intrusion-detection-systems-IDS

[28] Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J. (2019) Man-in-the-Middle-Attack: Understanding in Simple Words. *International Journal of Data and Network Science*, **3**, 77-92. https://doi.org/10.5267/j.ijdns.2019.1.001

[29] Merriam-Webster (n.d.) Public-Key. Merriam-Webster.com Dictionary.

https://www.merriam-webster.com/dictionary/public-key

[30] Pavlyushchik, M.A. (2014) U.S. Patent No. 8,713,631. U.S. Patent and Trademark Office, Washington DC.

[31] Pavlyushchik, M.A. (2014) U.S. Patent No. 8,713,631. U.S. Patent and Trademark Office, Washington, DC.

List of Abbreviations

***Advanced Persistent Threat* (*APT*).** "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)" [22].

Biometrics. "The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity" [23].

Botnets. "A botnet is a group of compromised computers under the control of an attacker" [24].

Defense in-depth. "Defense in-depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier" [25].

***Denial of service* (*DOS*).** "A denial of service attack is an attempt by multiple attackers to make a service unavailable to its users" [26].

Firewall. "A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules" [26].

Intrusion detection system. Host intrusion detection systems and network intrusion detection systems are methods of security management for computers and networks [27].

***Man-in-the-middle attack* (*MitM*).** "A kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users" [28].

***Hash Algorithm* (*Hash*).** "An encryption algorithm *set* of rules by which information or messages are encoded so that unauthorized persons cannot read them" [29].

Password. "A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user" [24].

***Public Key Infrastructure* (*PKI*).** "A cryptographic element that is the publicly shared half of an encryption code and that can be used only to encode messages" [30].

Phishing. "Phishing is the combined use of fraudulent e-mails and legitimate looking websites by cyber criminals in order to gain user credentials" [24].

Social Engineering. "Social engineering refers to psychological manipulation of people into accomplishing goals that may or may not be in the target's best interest. In cyber-attacks, it is often used for obtaining sensitive information, or getting the target to take certain action (e.g. executing malware)" [22].

Spam. “Spam is the use of e-mail technology to flood mailboxes with unsolicited messages” [24].

SQL injection attacks. “These consist of attacks against web applications with the aim of extracting data or stealing credentials or taking control of the targeted web server” [24].

Watering Hole Attacks. “The concept of a watering hole attack is similar to a predator waiting at a watering hole in a desert, as the predator knows that the victims will have to come to the watering hole. Similarly, rather than actively sending malicious emails, the attackers can identify 3rd party websites that are frequently visited by the targeted persons, and then try to infect one or more of these websites with malware” [22].

Worms/Trojans. “Worms and malicious programs have the ability to replicate and redistribute themselves by exploiting the vulnerabilities of their target systems” [24].

Zero-day Attacks. *“Z*ero-day vulnerabilities, i.e., threats that use an error or a vulnerability in the application or the operating system and arise immediately after the vulnerability is found, but before the relevant upgrade is issued” [31].