

Cyber Security Evaluation for a Petroleum Refinery Using Attack Tree Methodology and Economic Indexes

Koyejo Oduola^{1,*}, Ayoade Kuye¹, Fadilah Shehu²

Abstract

Information Technology (IT) is vital and valuable to our society. An important type of IT system is Supervisory Control and Data Acquisition (SCADA) systems. The most common misconception regarding the security of SCADA was that this network was electronically isolated from other networks and hence attackers could not access them. Over the years SCADA systems have become incorporated with other IT systems, which has made them becoming increasingly vulnerable to cyber threats. Decision makers should assess the security that the SCADA system's architecture offers so as to make notified decisions about its appropriateness. In this work a mixed qualitative and quantitative approach for evaluation of Cyber security for a Hypothetical Refinery. Cyber security scenario has been modeled by using Defense Tree (DT), an extension of Attack Tree (AT) with attack countermeasures. Numerical values were assigned to the leaf nodes to assert the difficulty of compromising the root node and quantitative indexes for computing the defender's Return On security Investment (ROI) and the attacker's Return On Attack (ROA). It has been shown that this approach can be used to evaluate the strength and economic profitability of countermeasures as well as their impediment effect on attackers, thus providing decision makers with a utilitarian tool for performing better evaluation of Cyber security investments during the risk management process in our local refinery.

Keywords: SCADA, Vulnerability Assessment, Attack Tree, Defense Tree, ROA, ROI

INTRODUCTION

The widespread introduction of digital network systems in refineries has increased such infrastructures vulnerability to cyber-attacks. Also in recent years, the world has become more and more connected via the Internet. Although this has brought great convenience and many new technological opportunities, it has also brought along new possibilities for criminals in the form of cybercrime. This called for the need of cyber security, which is defined by the Merriam-Webster dictionary as "measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack".

*Author for Correspondence

Koyejo Oduola

¹Senior Lecturer, Department of Chemical Engineering,
University of Port Harcourt, Nigeria

²Professor, Center for Gas, Refining and Petrochemicals,
University of Port Harcourt, Nigeria

Received Date: March 01, 2021

Accepted Date: May 20, 2021

Published Date: May 29, 2021

Citation: Koyejo Oduola, Ayoade Kuye, Fadilah Shehu. Cyber Security Evaluation for a Petroleum Refinery Using Attack Tree Methodology and Economic Indexes. Emerging Trends in Chemical Engineering. 2021; 8(1): 20–29p.

Over time the number of attacks performed has increased tremendously and attacks are becoming more and more complex [1]. There are estimates that say that in 2013 there were more than 800 million incidents and the economic impact of cybercrime is estimated to \$400 billion per year [2]. These numbers emphasize the need for effective cyber security efforts.

Major problems are that IT security experts are often tied to strict budgets [3], which means that decisions will have to be made on which measures to take. Also the IT security experts often do not have a very good insight in the cyber threats that

exist, which is as a result of communication gaps between security managers and IT managers, resulting in decisions that do not fully take into account both the economic convenience and the technical effectiveness. In order to help IT security experts to take the right decisions and to give them more insight in the cyber threats they are dealing with, tools have been developed. One of such tools is the Attack Tree methodology, which is the focus of this research. In 1999, Schneier popularized attack trees as a tool to evaluate the security of complex systems [4].

With the use of the attack tree methodology, attacks can be seen as games between the attacker and the defender. Attackers are often assumed to behave rational, which means that they will only attack when an attack has a positive expected outcome [5] (Buldas et al., 2006). For the defender the goal is to make sure there is no profitable attack possible on the system. The objective of this research is to design a framework in which the motivation of the attacker is included in the attack tree methodology. By so doing, the attack tree methodology can be used to analyze the security of a system for different types of attackers in terms of what motivates them to perform an attack. This will provide the IT security expert with a better insight on possible attacks that may be performed, help the IT security expert to determine where to take countermeasures and thus model a Defense Tree.

The attack tree methodology was founded by Weiss [6]. He introduced a system security engineering process to help allocate resources to vulnerabilities with the highest risk. In his method he used a tree like structure to decompose threats, which he named threat logic trees. The name attack tree was first used by Schneier [7] who described the process of setting up an attack tree and allocating parameters to the attack tree to answer various questions about the security of a system.

Intrusion Detection Systems (IDS) had been in existence for over two decades ago, starting in 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance. Several commercial investments have emerged for developing IDS such as Intrusion Detection Systems for Computer Networks and Snort-Lightweight Intrusion Detection for Network. However, technology has been limited to provide a cost-effective model. In this decade, several algorithms have been developed for encryption, decryption, public key exchange, secure socket layer, and digital signature. These algorithms help to improve IDS technology as well [8, 9].

Tanya et al. [10] in their work showed that Model-based IDS can be useful in detecting unknown attacks. They used the peculiar characteristic of the SCADA to find the main goal of the attacker, which is to compromise the availability, and integrity of gathered data.

Jones and Horowitz [9] provided an application example focusing on addressing the threat of cyber attacks against nuclear power plants, and outlined an initial vision for a security analysis framework to compare alternative security architectures. A lot of works have been done over the years on Industrial Cyber Systems; Attack tree methodology, Defense in-depth, Smart grid. This work therefore attempts to apply these methodologies to our local refinery in Nigeria.

METHODOLOGY

Attack trees are models of reality. They are a simplified representation of complex real world drivers. The attack tree models provide insight into the attack methodology. The model displays step-by-step methodology involved in carrying out an attack successfully [11].

There are two possible approaches that the security risk management process can follow: the qualitative and the quantitative approach. The qualitative approach is centered on comparative evaluation of risks. The quantitative approach [12] (Meritt, 1999) assigns absolute numeric attribute values to assets, threats, vulnerabilities and countermeasures. The exact identification of risk and the cost/benefit justification of countermeasures are fundamental for constructing a good risk mitigation strategy.

Cremonini and Martini [13] proposed using the ROA and the return on investment (ROI) to measure how the attacker's preference changes with the selected security measure. This work compares the capital invested on the security apparatus and the gains from such investments. It reveals the cost implication and possible profit from some security investments. The qualitative approach was used to model security scenarios, via a modified version of attack trees, that is the defense tree and hence compute the Return On Attack (ROA). Quantitative indexes have been used to measure risk, Return On Investment (ROI).

An Attack Tree was constructed by which equipment could be destroyed; by consulting experts in the field and also with the use of SecurTree (a software which can draw attack tree and also defense tree). The tasks needed to achieve the success of the attack (to compromise the root node) must be performed simultaneously as presented in Figure 1.

Return On Attack (ROA)

The ROA has been employed in this work as given by Akinola et al. [14, 15]:

$$R = P_o C P_s \quad (1)$$

Where, P_o = payoff

C = commitment;

P_s = probability of success

The payoff values range from 1 to 10 and are classified as shown in Table 1 [16]. L, M, H and VH represent Low, Medium, High and Very High, respectively.

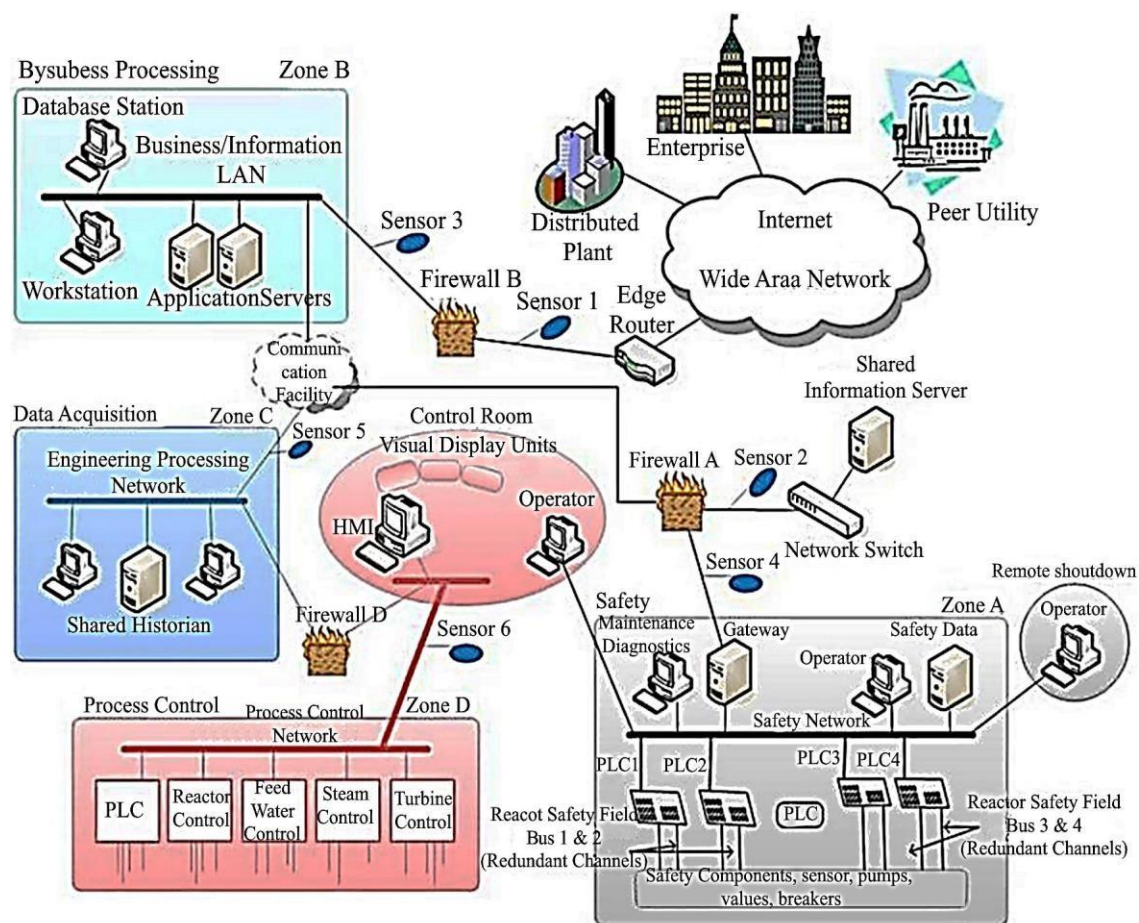


Figure 1. A Network Diagram of Hypothetical Nuclear Power Plant [14].

Table 1. Quantifying Attack Payoff [16].

Numerical Range	Payoff Definition
1–3 L	Minor impact to the system. Attack could be easily detected and/or repaired.
4–6 M	Moderate impact to the system. There is reduced performance or interruptions in resource availability. Integrity, confidentiality and availability of the system affected. Requires special effort to detect and/or repair.
7–9 H	Severe impact to the system. Significant damage results to the system. There are considerable informational disclosure and access to some system files. Considerable efforts are required to detect and/or repair the damage.
10 VH	System completely compromised, inoperable or destroyed. The attacker can render the resource completely unavailable.

The probability of success is calculated using the equation:

$$Ps = Acv * Ca * Au \quad (2)$$

Where, Acv = Access vector

Ca = Access complexity

Au = Authentication

The access vector (Acv) shows how vulnerability may be exploited. The access complexity (Ca) metric describes how easy or difficult it is to exploit the discovered vulnerability. The authentication (Au) metric describes the number of times that an attacker must authenticate to a target node to exploit it.

The intermediate and root nodes Po and Ps are calculated using these equations.

For AND nodes:

$$Ps = \prod_{i=1}^K Prob_i \quad (3i)$$

$$Po = \frac{10^k - \prod_{i=1}^K (10 \dots ND \text{ nod})}{10^{k00}} \quad (4i)$$

For OR nodes:

$$Ps = 1 - \prod_{i=1}^K (1 - Prob_i) \quad (3ii)$$

$$Po = \max_{i=1}^K Payoff_i \quad (4ii)$$

Where, $Prob \in (0,1)$; $Payoff \in [1, 10]$;

K = number of leaf nodes [14]

The quantitative approach [12] assigns absolute numeric attribute values to assets, threats, vulnerabilities and countermeasures. Within this approach indexes from Bistarelli et al. [17] were used.

$$\text{Single Loss Expectancy} \quad SLE = AV \times EF \quad (5)$$

Where, the *Asset Value* (AV) is a synthetic measure of the cost of creation, development, support, replacement and ownership values of an asset. The *Exposure Factor* (EF) represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat event, and is expressed as a percentage of the asset value.

Annualized Loss Expectancy, (ALE) is the annually expected financial loss of an organization which can be ascribed to a threat and can be computed by using the following formula:

$$ALE = SLE \times ARO \quad (6)$$

Where the Annualized Rate of Occurrence (ARO) is a number that represents the estimated number

of annual occurrences of a threat. For this work ARO is taken to be 1 for all counter measures, this was because there are no data available to estimate this information correctly and industries are skeptical on this kind of data [17].

Return On Security Investment (ROI)

The Return on Security Investment (ROI) index is defined as: [17]

$$ROI = \frac{ALEa - (ALEa(1 - RMc)) - CSIC}{CSIC} \quad (7)$$

Where RM is the risk mitigated by a countermeasure and represents the effectiveness of a countermeasure in mitigating the risk. CSI is the cost of security investment that an enterprise must sustain for implementing a given countermeasure [17].

We describe the defender's point of view by enriching the given tree using economic quantitative labels that can help determine countermeasures to be selected for implementation taking into account the organization's return on investment. For each asset we want to protect, we proceed as follows:

- First, we consider-for each possible attack represented as a path in the tree-the Exposure Factor (EF) and the Annualized Rate of Occurrence (ARO); this part is very important because using incorrect data could lead to unexpected results;
- Then, we obtained the Asset Value (AV) as the Damage cost given by SecurItree for each node, and we compute the Single Loss Exposure to a threat (SLE) and the Annualized Loss Expectancy (ALE) for each leaf in the defense tree. In particular, when the last node before the leaves is an and-node, the computation of SLE and ALE is done considering the EF and ARO.
- Then, we consider the cost of each countermeasure (CSI) and the percentage of Risk Mitigated (RM);
- Finally, we compute the Return on security Investment (ROI) for each countermeasure. We can use ROI to match economic profitability of the different countermeasures that an organization can use to protect its own systems. For example, for each attack node, we could select the countermeasure, which maximizes ROI among all countermeasures, which are associated to its vulnerability nodes.

RESULTS AND DISCUSSION

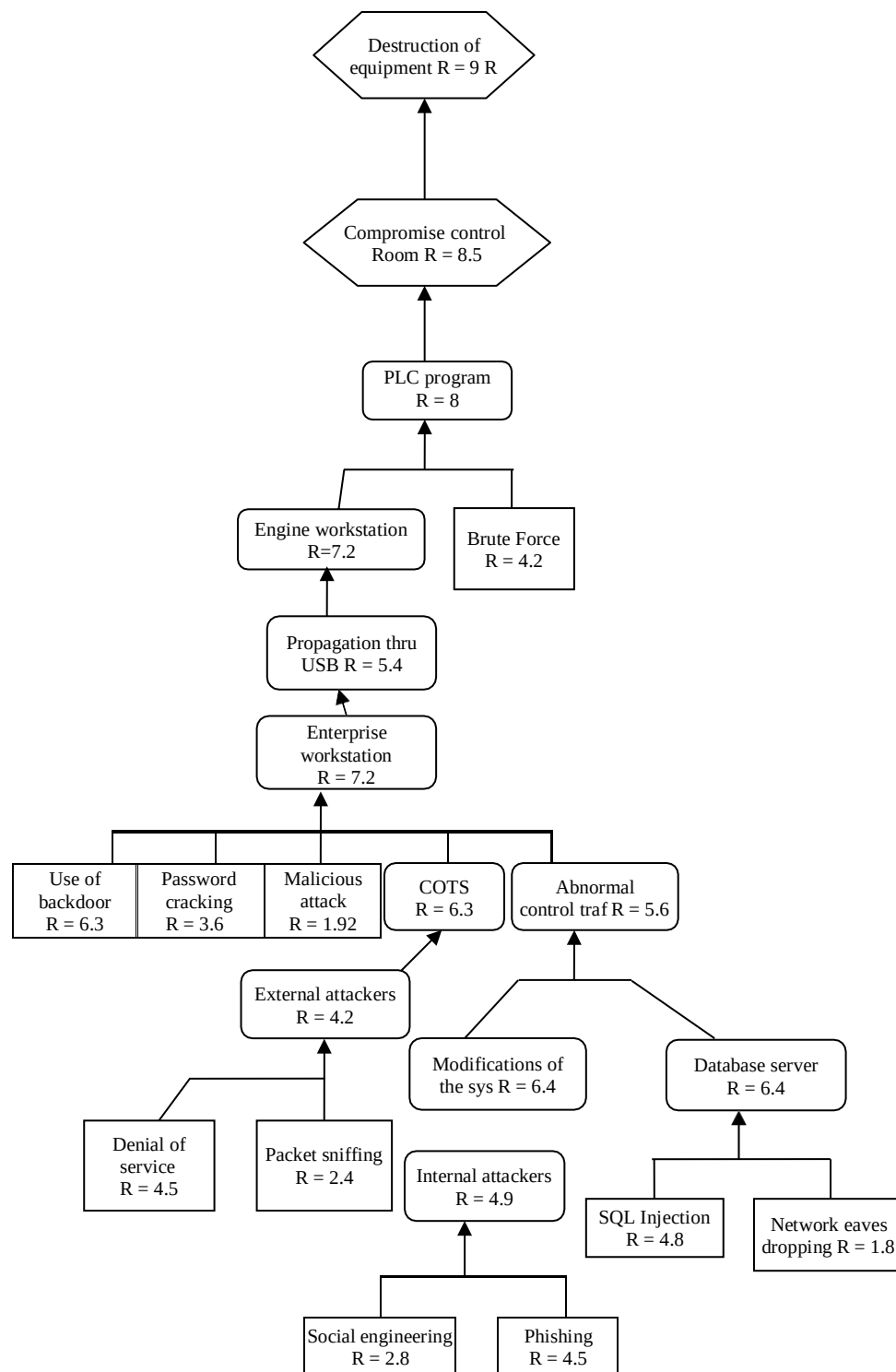
For the attack tree in Figure 2, the payoff, access vector, access complexity and authentication values are obtained from experts in the field. These are presented in Table 2. These values are used to calculate the ROA values for the leaf and intermediate nodes, required to compromise the control room for attack tree as shown in Figure 2.

Figure 2 shows that for the attack tree, the maximum and minimum ROA values are 9.0 and 1.8 when the access vectors, access complexities and authentication values are varied randomly within +50% of expert opinion. Clearly the ROA value at the root node indicate that the vulnerability of the control room can be exploited easily since this value fall in the high range as defined in Table 1.

Table 2. Data Used to Calculate the ROA for Attack Tree.

Node	Task Name	Po	Acv	Ca	Au	Ps	C
LN1	Social Engineering	7	1	0.4	1	0.4	1
LN2	Phishing	5	1	0.9	1	0.9	1
LN3	Network Eaves Dropping	3	1	0.6	1	0.6	1
LN4	SQL Injection	8	1	0.6	1	0.6	1
LN5	Packet Sniffing	4	1	0.6	1	0.6	1
LN6	Denial of Service	5	1	0.9	1	0.9	1
LN7	Malicious Codes Attacks	8	0.4	0.6	1	0.24	1
LN8	Password Cracking	6	1	0.6	1	0.6	1
LN9	Use of backdoor	7	1	0.9	1	0.9	1

Node	Task Name	Po	Acv	Ca	Au	Ps	C
LN10	Brute Force Attack	6	1	0.7	1	0.7	1
AN1	Internal attackers	7	1	0.7	1	0.7	1
AN2	Database Server	8	1	0.8	1	0.8	1
AN3	Modifications of the system	8	1	0.8	1	0.8	1
AN4	External attackers	7	1	0.6	1	0.6	1

**Figure 2.** Attack Tree.

A defense tree was built as shown below from securITree, with the necessary counter measure required at each leaf node. It should be noted that counter measures could only be applied at the leaf nodes. Intermediate and root nodes do not carry counter measure, even though its presence at their leaf nodes would also affect them. The ability of countermeasure to mitigate attack or vulnerability was obtained from literature and expert opinion. This was used to calculate ROAc values as shown in Table 3 (Figure 3).

From the defense tree the security manager can already make several considerations, to mitigate all the attacks, at least one countermeasure has been selected for each path. The countermeasure with highest ROI is selected (in fact, the higher the ROI the better the investment). So, for this study the best countermeasure seems to be the installation of anti-virus software with ROI 38.2.

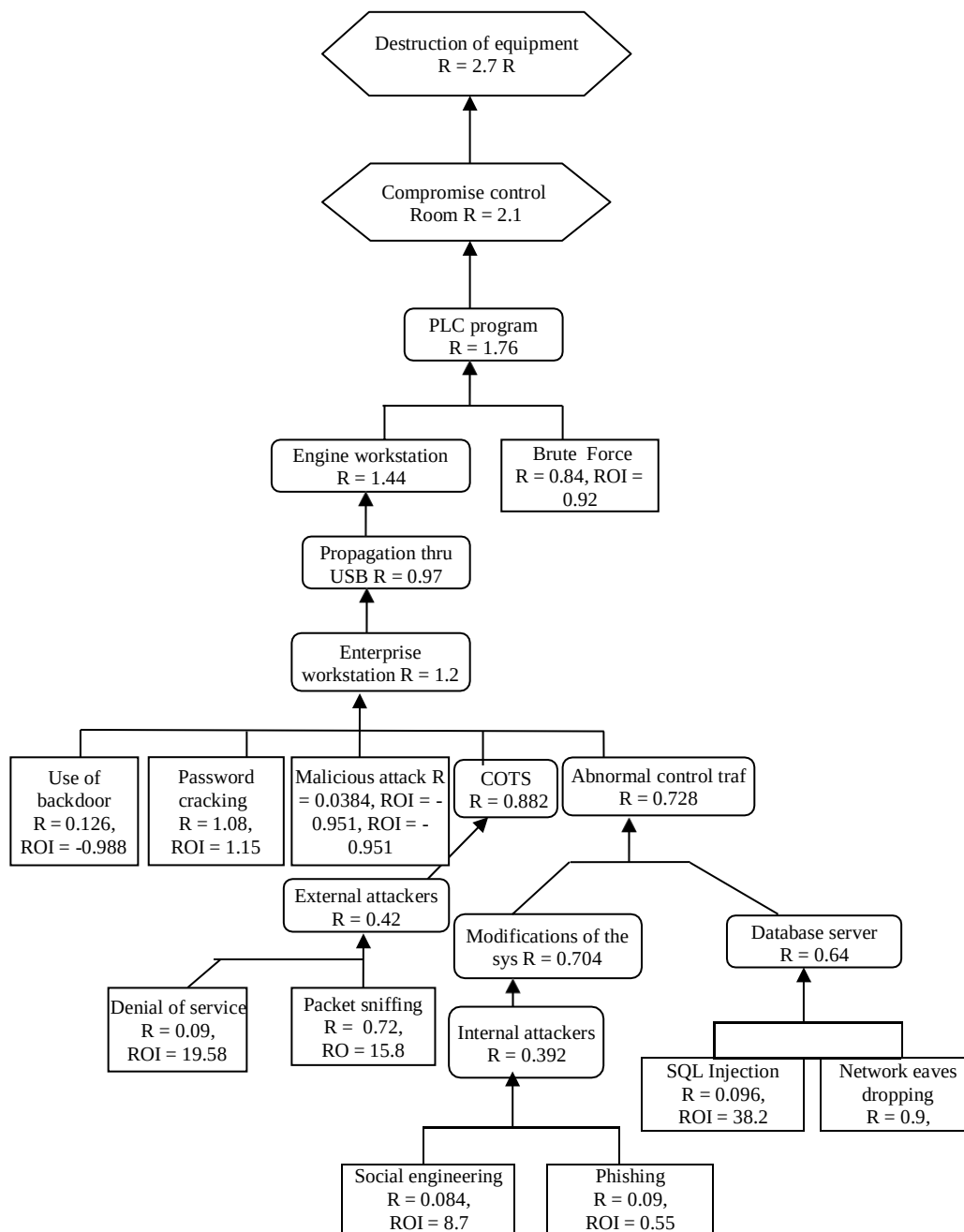
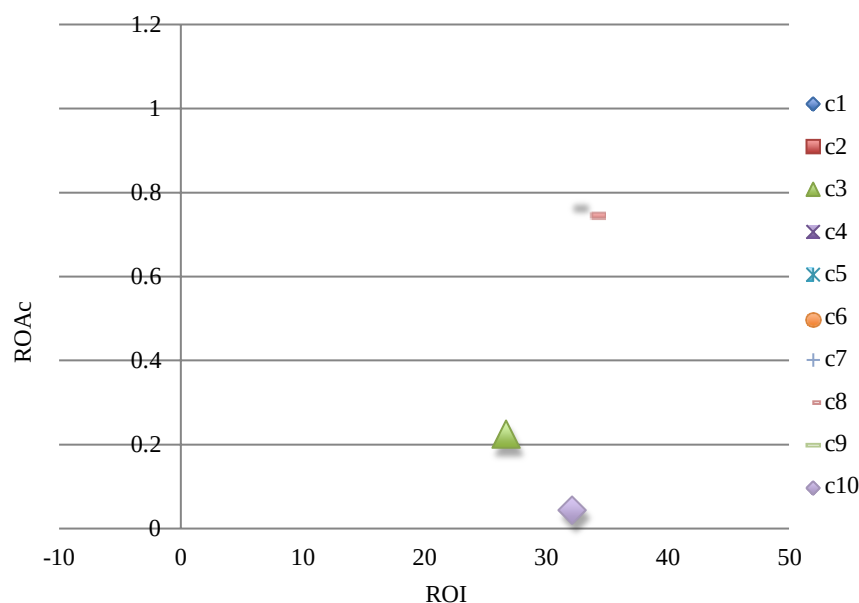


Figure 3. Attack Treewith ROAc and ROI.

Table 3. Data Used to Calculate the ROAc for Attack Tree.

Node	Task Name	Counter Measure	RMc	1-RMc
LN1	Social Engineering	Firewall	0.97	0.03
LN2	Phishing	Anti Virus Software	0.98	0.02
LN3	Network Eaves Dropping	Encryption	0.5	0.5
LN4	SQL Injection	Anti Virus Software	0.98	0.02
LN5	Packet Sniffing	Access Control, IDS	0.7	0.3
LN6	Denial of Service	Firewall, IDS	0.98	0.02
LN7	Malicious Codes Attacks	Anti Virus Software	0.98	0.02
LN8	Password Cracking	Access control, Authentication of IP address	0.7	0.3
LN9	Use of backdoor	Firewall, IDS	0.98	0.02
LN10	Brute Force Attack	Access Control, IDS	0.8	0.2

**Figure 4.** The ROI and ROA associated with each possible set of countermeasures when it is used to mitigate the risk produced by all the possible attacks.

When the process of labeling the considered defense tree with ROI and ROA is complete, we put together those indexes and perform a synthetic evaluation so as to determine the security investment that provides the best return on investment and that discourages the attacks best.

The risk management process team should ideally select a countermeasure maximizing ROI and minimizing ROA. When such a countermeasure does not exist a countermeasure should be selected that either:

- Maximizes ROI or minimizes ROA,
- Is any Pareto-optimal countermeasure, or $c_{\text{sep}}^{[1]}$
- Maximizes a user-defined function of ROI and ROA. [17].

Figure 4 shows the defense tree labeled with both ROI and ROA. The double labeling gives the security manager the complete view of the scenario. The first step is the elimination of countermeasures dominated by some other and concentrate on the Pareto-optimal.

To do this we build a graph for the attack, where all countermeasures are compared with their respective ROA, as shown in Figure 4.

CONCLUSION

This work considered an attack scenario to disrupt equipment by compromising control room of a hypothetical network refinery and quantitatively evaluates the network security using an attack tree model. Using the developed models, the calculated ROA for the attack scenario was high. This means that the control room can easily be compromised and hence leads to equipment disruption. When a defense tree was modeled by implementation of suggested upgrades, the ROA values reduced to 2.7. The model can, therefore be used to quantify the vulnerability of computer network. When both ROI and ROA were plotted on a graph it was observed countermeasure Counter measures 1, 2, 6, 7 and 9 (represented as c1, c2, c6, c7 and c9 on Figure 4 above) have very low ROI and low ROA. Counter measures 3, 8 and 10 (represented as c3, c8 and c10 on Figure 4 above) have low ROI and very high ROA. This is clearly for the attackers' benefit. Counter measure c4 has the highest ROI value of 38 and smaller ROA value of 0.096.

The first thing done was to eliminate, if any, sets with a negative value of ROI, as they do not represent profitable investments. Then, we discarded dominated sets in such way that only the Pareto-optimal solutions are considered. At this step some countermeasures can be discarded. If the security manager wants to maximize ROI and minimize ROA, then countermeasure 4 (Anti virus software) will be selected, whilst if he/she prefers to minimize ROA, the selected countermeasure will be 7 (Anti virus software). In this work the main aim is to maximize ROI and minimize ROA therefore, we choose counter measure 4, because it gives us a profitable investment and a secured system.

Limitations and Recommendations

The major limitation was in obtaining reliable data to be used, most data were obtained from experts' opinion. ARO of attacks can be tricky to estimate, because organizations are typically reluctant to make attack data publicly available as this can have a negative influence on their reputation. The use of questionnaire can help have a statistical evaluation to some of this data needed for this research work and also a creation of database where this information can be easily accessed.

The methodology presented in this article provides a basis for future work along several research directions. We plan to investigate how to leverage existing results on constraint semirings and their use in attack trees rewriting [18] for computing attribute values of AND/OR nodes as functions of attribute values of their children in the considered defense tree. Results borrowed from probability [19] and possibility theory [20]. Dubois & Prade [21] can also be useful for estimating frequency and likelihood of attacks from frequency and likelihood of vulnerabilities used in the attack.

Thus, another interesting direction of research may consist in exploring how ROA and other information about the attacker, like, for example, non-economic motivation, risk attitude and type of attackers (which can range from script-kiddies to organized crime and cyber terrorist), can influence the ARO of attacks, also from a game theoretical perspective.

Other interesting extensions to the work presented in this article include considering how vulnerabilities can be used for attacking multiple assets of an organization, how to replace fixed attribute values with constraints (e.g. intervals), and how to use fuzzy logic techniques to define functions combining ROI and ROA indexes.

REFERENCES

1. VanKessel P. and Allan K. (2013). Under Cyber Attacks.:*Global Information Security Survey(online)*. Available from <https://www.slideshare.net/ernstandyoung/under-cyber-attack-eyes-global-information-security-survey-2013-30942141>
2. McAfee. (2014). Net Losses: Estimating the Global Cost of Cyber Crime, Economic Impact of Cyber Crime: *Center for Strategic and International Studies(online)*. Available from https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

3. VanKessel P. and Allan K. (2014, October). Get Ahead of Cyber Crimes: *Global Information Security Survey*(online). Available from <https://www.eycom.ch/en/Publications/20141125-Get-ahead-of-cybercrime-EYs-Global-Information-Security-Survey-2014/>
4. Barbara K., Sjouke M., SasaR., et al. Attack-Defense Trees. *Journal of Logic and Computation*. 2012; 24(1): 55-87.
5. Buldas A., Laud P., Priisalu J., et al. Critical Information Infrastructures Security: Rational Choice of Security Measures via Multi-parameter Attack Trees. Berlin, Germany: Springer Berlin Heidelberg; 2006.
6. Weiss, J. D. (1991). *Proceedings of the 14th National Computer Security Conference: A system Security Engineering Process*; 1991 October 1-4; Washington DC: National computer security center; 1991.
7. Schneier, B. Attack Trees. *Dr. Dobb's Journal*. 1999; 24 (12): 21-29.
8. Hossein Bidgoli, editor. *The Handbook of Computer Networks: Denial of Service Attacks*: California; John Wiley & Sons. 2007.
9. Horowitz B., Jones R. A. A system aware Cyber Security Architecture Systems and Information Engineering. *Systems Engineering*. 2012; 15 (2): 225-240.
10. Tanya R., Dennis N., Ulf L., and et al. Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2008): An Intrusion Detection System for Wireless Process Control System; 2008 Sep29-Oct 2; Atlanta. US: IEEE; 2008. 866-872.
11. Amenaza. (2005). Fundamentals of Capabilities based Attack Tree Analysis (online). Available from <https://www.amenaza.com/downloads/docs/AttackTreeFundamentals.pdf>
12. Meritt, J.W. (1999). A Method for Quantitative Risk Analysis Approach, CISSP, WLNG GLOBAL(online). Available from <https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p28.pdf>
13. Cremonini M, Martini P. (2005, June). Evaluating Information Security Investments from Attackers Perspective: the Return On Attack (ROA) (online). Available from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9925&rep=rep1&type=pdf>
14. Akinola A., Kuye A., Ayodeji A. (2014). Cyber Security Evaluation for a Hypothetical Nuclear Power Plant using Attack Tree Methodology. *Journal of Nuclear Engineering and Technology*, 4 (1).
15. Akinola A., Kuye A., Ayodeji A. *Proceedings of the 55th Annual Meeting of the Institute of Nuclear Materials Management (INMM): Cyber Attacks Analysis of a School Network*; 2014 July20-24; Atlanta, Georgia. NY: Curran Associates, Inc.; 2015.
16. Edge K., Raines R., Baldwin R., et al. Analyzing Security Measures for Mobile Ad hoc Networks Using Attack and Protection Trees. *Journal of Information Warfare*. 2007; 6(2): 25-38.
17. Bistarelli S., Fioravanti F., Peretti P. First International Conference on Availability, Reliability and Security (ARES'06): Defense Trees for Economic Evaluation of Security Investments. 2006; Vienna, Austria. US: IEEE; 2006. 426-423.
18. Mauw S., Oostdijk M. *8th International Conference on Information Security and Cryptology: Foundations of Attack Trees*; 2005 December; Berlin, Heidelberg: Springer-verlag; 2005.
19. Lindley D.V., Hoboken N.J. *Making Decisions*. 2nd ed. London: John Wiley and Sons; 1985.
20. Zadeh, L.A. Fuzzy Sets as a Basis for a Theory of Possibility. *Fuzzy Sets and Systems*. 1978; 1(1): 3-28.
21. Dubois D., Prade H. Possibility Theory: An Approach to the Computerized Processing of Uncertainty. 1st. ed. Germany: Springer; 1988.