The Framework for Information Security Risk Network Management based on Bayesian Belief Decision Support System for Threat on the Campus

*Aliyu Mohammed, Sulaiman Mohd Nor, Muhammad Nadzir Marsono
*Department of Microelectronic and Computer Engineering
Universiti Teknologi Malaysia Faculty of Electrical Engineering

Abstract

The security network management system is for providing clear guidelines on risk evaluation and assessment for enterprise networks. The risk evaluation is based on the relationships among the most critical assets, and threats that are likely to those assets and their vulnerability impacts. Threat and risk assessment are conducted for identifying the safeguards to be adapted in order to maintain system confidentiality, integrity, and availability through effective control strategies. In this paper, we provided an integrated information security decision management analysis and an articulated understanding of the risks due to malware propagation on the campus network. The developed Bayesian Belief Network decision support system along with inference level indicator will enable the decision maker to understand and provide appropriate decisions for mitigation and control countermeasures for the organizations infrastructural assets being at risk. We experimentally placed monitoring sensors on the campus network that gives the threat alert priority levels and magnitude on the vulnerable information assets. These will give a direction on the belief inferred due to malware prevalence on the information security assets for better decision making on control strategies

Key words: Network security; malware propagation; Bayesian Belief Network; control and mitigation strategies

INTRODUCTION

Broadly available malicious software (adware and spyware) affect users' productivity, compromise their privacy, and modify (damage) system assets. We determine relations between the infection distribution and also the status of the infected system to estimate the general effect on the enterprise network. The Methodology presented within this paper determines and discusses the following concepts:

Infection and probability occurrence triggered by malware. Risk computation with uncertainty compensation of infection and recovery models based on Bayesian Belief Network. Control measures and loss functions of recovery facilities based on the assets.

The prevalence of malware propagation on the internet and the campus network has caused loss of data and vital information estimated to be in the tune of some thousands of dollars for most enterprises. The experts in the information security stated data breaches are inherent costs of doing business online. Organizations take necessary steps to safeguard customer information to provide proper risk management processes that are carried out should a data breach occur. The Federal Trade Commission (FTC - US) filed suit against hospitality giant Wyndham Worldwide in June 2012 for exposing 619,000 consumer payment account information's to a domain in Russia. The FTC claims that defendants' failure to maintain reasonable security allowed intruders to obtain unauthorized accesses resulting in $10.6 million in fraudulent charges as far back as 2008, according to court documents.

The FTC stated that identity theft and other forms of crime cost Americans $1.52 billion in 2011, reported by Reuters, and all efforts are to reduce such theft. In essence, most of the complaints filed with the FTC are identity-related crimes ranging to1.8 Million. This was twice what was obtained in 2006. *Aberdeen Group* an information technology research firm provided that worldwide effect of identity theft is an about $221 billion drain on businesses. *Ponemon Institute* an independent privacy policy research center came up with a report that the annual cyber crime costs for the affected organizations which ranges between $1 million to $52 million. The second annual report of "*Cost of Cyber Crime Study''*, the center indicates that most costly cyber crimes caused by malicious code, DoS (denial of service), stolen devices, and Web-based attacks. Most of the attacks are as a result of malicious activities like stealing intellectual property, hijacking online bank accounts, and creating and distributing viruses on computers. It also includes aspects like posting confidential business information on the Internet and even disrupting critical national infrastructure. Although most organizations do not present the actual position of their compromised data, thus it makes it difficult to calculate the accurate damage and loss[1]. While tightening email security screws is useful, there is growing concern that cyber criminals will turn their focus on other popular technologies, example mobile products and social networking sites. Using the proliferation of social networking, mobile products, and location- based services, experts agree that the playing ground for cyber thieves has increased. The increased high level of data on the network is the main reason."Think about your Facebook profile and how many data the company has based on what have shared [and what others share about others]," "These profile is to stored, secured, and high privacy policies applied. Facebook's valuation depends on that richness of data."

Bayesian Belief Network provides the understanding to enable for containing the propagation of the malware. The BBN has both the quantitative and qualitative ability to measure the prevalence of the malware risk factor on the vulnerable assets. The BBN based on decision support system is a tool that can relate and give the causal relationships that exist between risk factors, some risk key indicators with their associated operational attributes. The tool can effectively perform inference reasoning and predictions under some predefined scenarios. BBN is a probabilistic cause- effect model or probabilistic influence diagram that describe the probability distributions about sets of variables by indicating their conditional independence assumptions along with their conditional probabilities [2].

The paramount question always asked is how do we effectively understand the magnitude of the malware propagation and prevalence on the network assets? How do we present a clear and understandable risk assessment to the decision maker for easy decision? To find solution to these questions we need to look at the inner operations of BBN and the enterprise risk assessment and evaluation with a view to understand the effects of malware prevalence on the network assets.

Risk assessment handles the valuation of recent risk factor status, considering their probability and consequence. This issue may be used from the quantitative scoring method and also the probability presented by considering Bayesian network. The value of diagnostic reasoning is the facts that once the enterprise value level is high, we are able to infer the prospective degree of factors that are mounting on the enterprise value. The greater it is an indicative of the long run direction of risk management. In

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

comparison to traditional risk assessment techniques Fault trees, Bayesian Systems give a superior modeling way of dynamic risk analysis and assessment. The virtues of Bayesian Network model are its inference engine for upgrading the posterior possibility of enterprise value given new information or key risks is high. It suggests that Bayesian Network model allows the organization to have various choices in the network structure, even with the addition of an auxiliary node. This probability upgrading not just continuously cuts down on the data uncertainty, it offers the enterprise risk scenario with real-time and up-to-date analysis[3].

The composite concept for the generation of attack data as well as connected risk assessment approach utilizing a homogeneity method for fast evaluation of large system. Instead of testing each resource individually by using repetitive attacks and checks again and again, the composite concept creates and executes attacks once for some assets. The qualities of risk data are for assessing the remaining assets with other network facilities will provides a unique system approach[4]. The lifecycle information security risk assessment techniques are required for guidance before beginning a risk assessment process. At the moment, there is virtually little formal guidance regarding how to utilize Bayesian Belief Network (BBN) inference using both available data and evidence information on malware prevalence on the network infrastructure. However, there is an increasing curiosity about how we can apply Bayesian Network (BNs) using both data plus some evidence information to understand the magnitude of malware propagation prevalence and damages to network infrastructure[5]

A good example of decision analysis of statistical distribution denial-of-service (DoS) flooding attacks is presented by Li et.al[6]. However, such approaches using BBNs towards the analysis of network security risk propagation are difficult to come by in the literature.

The remainder of this paper is structured as follows. Section II describes the basic principles of Bayesian Belief Network (BBN). This includes the probabilistic conditional inferences and decision making analysis. Section III we discuss the use of Bayesian Belief Network and its application towards the malware prevalence on the network. Section IV suggests controls measures and mitigation strategies. Finally, some concluding remarks in section V.

2. THE BAYESIAN NETWORK PRINCIPLES

2.1. The essence of Bayesian Rule

The Bayesian approach provide mathematical rule explaining how it should change belief with new evidence. Meaning that, it allows researchers to combine new data with knowledge and ability. The clear example imagining that a precocious newly born observes the sunset and wonders if the sun will rise again. The given equal prior probabilities for possible outcomes are represented by placing white and black marble inside the container. The next day the sun rises and young teenager inserts another white marble in the container. The probability that a marble plucked randomly from the bag will be white (i.e., the child's degree of belief in future sun rises) has thus gone from a half to two-thirds. The day youngster adds one more white marble, and the probability (and thus the degree of belief) increases to three-

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

quarters. Ultimately the belief that the sun is likely not to rise each morning will change to a complete certainty that it will all the time rise.

Mathematically, the Bayes' rule states: $Posterior = \frac{Likelihood * prior}{m\arg inal \cdot likelihood.}$,

Symbolically it can be represented as - $P(R = r \mid e) = \frac{P(e \mid R = r)P(R = r)}{P(e)}$ (1)

Where $P(R = r \mid e)$ denotes the probability that random variable R has value r given the evidence e. The factor in the denominator is just a normalizing constant that ensures that the posterior adds up to 1. These are computed by summing up the equation at the numerator over all values:

$$P(e) = P(R = 0, e) + P(R = 1, e) + ... \\ = sum \cdot rP(e \mid R = r)P(R = r) \quad (2)$$

This procedure becomes the marginal likelihood (as we have marginalized out over R) and provides the prior probability of the evidence. Thus, the concept of the child, parent, consequence and the conditionality's are as depicted through the deduction and abduction process shown in Figure 1.

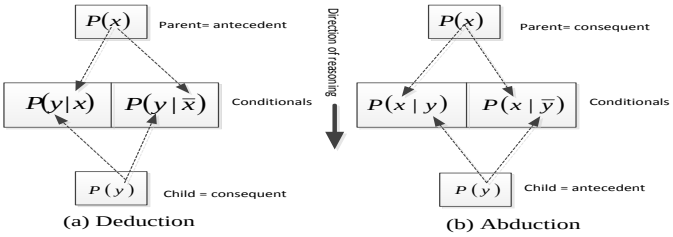


Figure1. The concept of deduction and abduction probability[7] [adapted from Josang, A]

2.2. Probabilistic Conditional Inference

The assertions of conditional propositions like `IF x THEN y' is the fact that once the antecedent is false, it is impossible to say the reality about the consequent. Precisely, what it takes is a complementary conditional that will covers the situation once the antecedent is false. Once that is appropriate, it may be the conditional `IF NOT x THEN y'. With this conditionality; it is possible to look for the truth that is worth the consequent y in case the antecedent x is false. Each conditional provides an element of the complete picture and may be known as sub-conditionals. Together, these sub-conditionals form an entire conditional expression that delivers an entire description from the link between the antecedent and the consequent. Complete conditional expressions possess a two-dimensional truth value

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

simply because they contain two sub-conditionals that govern both their sheer own truth value. We adopt the notation y | x to convey the sub-conditional `IF x THEN y', (this in compliance with R.C. Stalnaker's [8] assumption that the prospect of the proposition x suggests y is equivalent to the prospect of y given x) and y | x to convey the sub-conditional `IF NOT x THEN y' and assume that it is significant to assign opinions (including probabilities) to those sub-conditionals. We think that the idea within the truth from the antecedent x and also the consequent y could be expressed as opinions. The conditional inference with probabilities is as related below:

Let x and y be two statements with arbitrary dependence, and let $\bar{x}$ = NOT x. Let x, $\bar{x}$ and y be related through the conditional statements y | x and y|$\bar{x}$, where x and $\bar{x}$ are antecedents and y is the consequent.

Let P(x), P(y | x) and P(y |$\bar{x}$) be probability assessments of x, y | x and y |$\bar{x}$ respectively.

The probability p(y || x) defined by:-

$$P(y \parallel x) = P(x)\,P(y \mid x) + P(\bar{x})\,P(y \mid \bar{x}) = P(x)\,P(y \mid x) + (1 - P(x))\,P(y \mid \bar{x}): \quad (3)$$

This is then the conditional probability of y as a function of the probabilities of the antecedent and the two sub-conditionals.

The essence of the notation y || x is to denote that the truth or probability of the statement y derived through antecedent together with positive (ve) and negative (-ve) conditionals. Therefore, the notational factor y || x is meaningful in the sense of probabilistic only, meaning that the factor P(y || x) represents the consequent probability.

Assuming x to be TRUE (i.e. P(x) = 1) and x $\longrightarrow$ y is also TRUE (i.e. P(y | x) = 1), we can then deduce that y is TRUE when P(y || x) = 1. In a situation when P(x) = 1, it is only the positive conditionals considered, whereas P(x) = 0 considered for the negative conditionals. In all scenarios, the two conditionals are necessary in determining the probability of y.

2.3. The Bayesian Belief Network

Decision theory complements reasoning under uncertainty by delivering a coherent framework to create the compliance while using preferences from the decision manager [9]. Decision described as irrevocable allocations of assets, as well as the preferences that dictate your decision process to represent the relative values the decision maker places on each possible outcomes of the decision. The aim is always to boost the expected utility or benefit triggered by a few decision. Decision theories provide an axiomatic reason for preference graphically by decision trees and influence diagrams. The primary focus from the decision tree is about the procedural areas of an evaluation. The influence diagram includes probabilistic dependencies between variables, such as the Bayesian belief network. However, influence diagrams contain decision nodes that provide choices and value nodes that provide utility measures.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

Although influence diagrams and Bayesian belief systems resemble, they are on two different problems. Influence diagrams are employed just like a graphical assistance to measure the interaction between various areas of a problem, whereas Bayesian belief systems employed to infer information from available data.

A Bayesian network consists of a graphical structure that encodes domain variables, were the qualitative and quantitative relationships between them, provides for the encoding probabilities over the given variable[10]. The Bayesian Network can be considered to involve the process of decisions with value and / or utility functions which tend to describe the preferences or wishes of the decision-maker. These conceptual models called Influence Diagrams. In D. Heckerman [11]: A Bayesian network considered set of variables $X = [X_1,\ldots, X_n]$ that relates to network structure S that tries to encode a set of conditional independent factors about the variables in X, and a set of P being a local probability distributions associated with each set of the variable. All together this set of components tends to define the joint probability distribution around X. Thus, the network structure enclosed by S called a directed acyclic graph (DAG). The nodes in S corresponding directly to the variables **X**. The factor Xi is to denote both the variable and its corresponding node, and pa_i represents the parents of node Xi in S including the variables that correspond to those parents. Conditional independencies in S encodes that there are no arcs that relate them. In S the joint probability distribution for **X** can be depicted by the equation:-

$$p(x) = \prod_{i-1}^{n} p(x_i \mid pa_i) \qquad (4)$$

The local probability distribution P is the term of the products in equation one above. It shows the pair of (S, P) are the joint distribution of p(x). These define the Bayesian Network as follows:-

$$BN = (S, P)$$

$$S = \{(X_j, X_i) \mid X_i \in X, X_j \in pa_i \} \qquad (5) \qquad P = \{p(X_i \mid pa_i) \mid X_i \in X \}$$

The Bayesian Belief network enables for representing the components of a complex probabilistic reasoning in an intuitive graphical format. These make understanding and communicating with the systems remarkably easy for the mathematically unsophisticated entities. The quantitative aspect of Bayesian Belief networks enables for accommodating subjective judgments (expert opinions) as well as probabilities that typically based on objective data[12]. Another important factor of the BBN is that, the arrows presented in the network represent real causal connections and not just the flow of information that occurs during reasoning. Each of the nodes in Bayesian network associated with a set of probability tables. The nodes represent the proposition of variables of particular interest and can be for discrete or continuous system. While the arcs in a Bayesian network specify the independent assumptions that are between the random variables, the network does also have some built-in independent assumptions

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

implied in the graphical representation. A causality network generally Bayesian network with some added properties that the parents of each node made as its direct causes. In general, we use the Bayesian network typically to compute all probabilities of interest since BN in X determines a joint probability distribution for **X**. For example, *P* (f | *a, b, c, d, e),* is the probability of *f* following the observations of the other variables *(a, b, c, d, e),* and can be computed as follows:

$$P(f \mid a,b,c,d,e) = \frac{P(a,b,c,d,e,f)}{P(a,b,c,d,e)} = \frac{P(a,b,c,d,e,f)}{\sum_{f'} P(f',a,b,c,d,e)} = \frac{\prod_{i=1}^{n} P(x_i \mid pa_i)}{\sum_{f'} P(f',a,b,c,d,e)} \quad (6)$$

2.4. Analytical Example of Bayesian Belief Network

Through the use of the Bayesian rules and its concepts as depicted in equations (1) and (2), we wish to take a critical look at a typical scenario of an infectious disease that is to be tested within a community as an example. Assuming a test for the disease as positive, what will be the probability that the actual individual tested does have the disease? The actual scenario will be highly dependent on the level of accuracy and sensitivity of the test and the knowledge (prior) probability of the disease.

Let $P(X = +ve \mid D = T) = 0.9$, given that the false negative derived from the situation is $P(X = -ve \mid D = T)$ at 10% and the associated false positive is at 10% equally.

Let $P(X = +ve \mid D = F) = 0.1$.

Let us assume that the particular disease is a rare case with $P(D = T) = 0.01$ meaning that it is at 1% level.

Let as consider the elements of the equation that relates to equation (1): X is the tests; T is for true, F for false, and D for the disease. This signifies that R in equation (1) is the same as D for the disease. The evidence ‘e’ is to be denoted by the test to be positive i.e. T = +ve.

$$P(D = T \mid X = +ve) = \frac{P(X = +ve \mid D = T) * P(D = T)}{P(X = +ve \mid D = T) * P(D = T) + P(X = +ve \mid D = F) P(D = F)}$$

$$= \frac{0.90 * 0.01}{0.90 * 0.01 + 0.10 * 0.99} = \frac{0.0090}{0.108} = 0.08333 \quad (7)$$

The level of positive test is 8.33% giving the probability that the person has the disease; this can be justified if we assume that there are about 1000 people in the given environment. We expect that 10 will have the disease and are likely to be positive. All the 10% of the other group tested positive accidentally, of all the group only 10 of them are likely to have the disease within the population; in

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

actual sense it will be 10/110 that are within the region of being positive to have the disease and it is going to be around 0.09.

It is also possible to ignore the prior to make the belief objective by having the following equation:

$$P(D=T \mid X=+ve)=\frac{P(X=+ve \mid D=T)*P(D=T)}{P(X=+ve)} = \frac{0.90*0.1}{0.90*0.1+0.1*0.01}=0.989 \qquad (8)$$

This result indicates the true positive of the entire test and relies totally on the belief of the way the disease will spread through the population.

3. USING BAYESIAN BELIEF NETWORK SYSTEM TO MODEL MALWARE RISK

The Bayesian Belief Network is an effective tool with adequate technique for modeling, measuring and to a certain extent managing the characteristics of malware propagation risk on the network environment of the campus information assets. This is achieved through the use of prior knowledge of the causal risk factors and the possible probabilistic reasoning concept of the systems. The scenario is typically represented in a form of an acyclic graph that consists of states of nodes and directed arcs. In a nut shell, the Bayesian Belief analysis is to allow for improving the prior determined factors values in the event of any additional information that is obtained about the variables in the network. This is for building the conditional probability table (CPT) to depict the situation in Figure 2. The conditional probability tables that are affixed to the random variables within the model might be estimated from collected record information where there are readily available. When such similar information's are not available, the tables could be built based on opinion results. Assets risk models might be readily developed utilizing a graphical Bayes internet editor like the GeNIe application program [13]. This type of model is as templates for the risk analysis engine since the risk model for the assets which are of the identical type with the new model analyzed similarly. Therefore, this system capacity allows the new tool to become flexible enough to accommodate changes occurring in components, technology, and environment; in addition to new threats that might arise once in a while. Meaning that the level of risk that prevails in any given situation determined both by the severity of the consequences arising from the occurrence of the risk event and the likelihood of its occurrence on the given asset.

Looking at a situation when a Trojan malware propagates through a network of nodes a model developed with the basic SIR model. The basic SIR is based on the typical model for epidemic modeling. Thus, the epidemic models are used to explain the rapid outbreak that occurs in an environment within a given time of less than one year; while it becomes endemic if it could extend to a longer time. This leads to a renewal of the susceptible in the system through births or recovery due possible temporal immunity. The thinking is that we are considering situation that the type of malware attack in the analysis is a single

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

type. This is just for the sake of simplicity of the analysis as it makes it easy to consider the rate of propagation and the possible recovery rate from the single malware type. The SIR (Susceptible, Infectious, and Recovered) nodes defines as; susceptible nodes are those hosts that their operating system; application and anti-virus not updated could be vulnerable to an attack by the virus; while infectious nodes are hosts that get infected when in an event of visiting malicious sites on the network and the malware is transferred to the host. Thus, the recovery nodes are hosts that are safe from a particular malware type but can still be susceptible for other malware on the network.

Looking at the SIR model, with the susceptible, infectious, and recovery host being at levels that are either high or low an indicated in the Figure 1 with given weightings based on the particular scenario. The conditional probability tables for each of the variables are conceptually given without particular evidence.

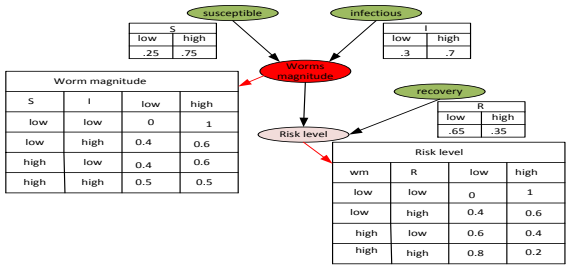


Figure2. Conceptual Conditional Probability Table (CPT) for SIR model.

The SIR factors (susceptibility, infectious and recovery rates) are measured per unit time; however the measurement could be per seconds, minutes, hour or days. When specific value is a signed to the measurements, make it discrete, as against continuous entity.

3.1. Probability Factor Analysis

Based on the conditional probability distribution of the causal variables in the SIR model, the likelihood occurrence for the magnitude of malware is determined due to the rate of infection and susceptibility when they are high given as 53%. Despite the fact that the recovery rate is low, the net effect of the risk has dropped to 51% yet is still high as indicated in Figure 3.

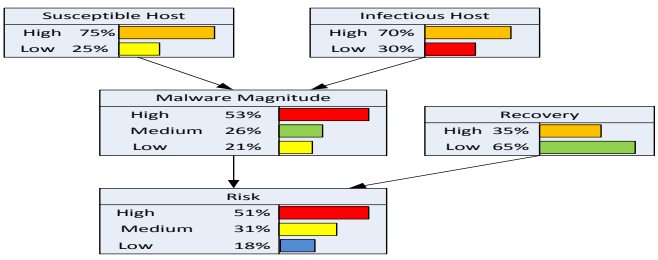


Figure3. Conditional Probability Estimation [13][*GeNIe 2007*]

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

3.2. Causal scenario analysis

The given scenario in Figure3 above shows that the model parameters are conceptual and the determination is based on fixing the values at wish and viewing the occurrence of the impact. In reality, the causal factor is through the provision of new evidence on the prevalence of the malware parameters. This parameter will then enable for updating and calculating the probabilities which is to be considered as the posterior probability analysis. This new information is to propagate to all the nodes on the network. The performance of the system tends to vary with the result of the new evidence provided, the rate of recovery does affect the overall risk even if the magnitude of the malware is at a high level. Thus, given the fact the susceptible and infectious nodes are low we have:

$$P(\text{magt.} \mid S_{low}, I_{low}) = 0.4 \; ; \; P(\text{Risk} \mid \text{magt. } 0.4, \text{Recv. } 0.9) = 0.51 \qquad (9)$$

This is evidently clear that the recovery does have an impact on the risk that is paused to the vulnerable assets on the network.

3.3. Malware Risk Propagation as a factor of Threat, Vulnerability, and Cost

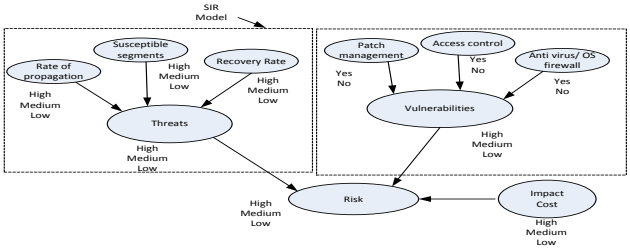


Figure4. Conceptual illustration of Risk Analysis as a factor of threat, vulnerability and cost (TVC)

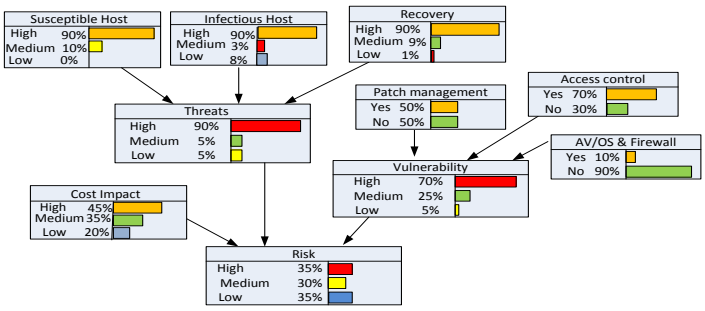


Figure5. Conceptual illustration of Risk Analysis as a function of threat, vulnerability, and cost with inference belief[13] [*GeNIe 2007*]

With the given structure and the associated variables explained, the associated conditional probability tables CPTs are as indicated in the Figure 5. Applying the principles of Bayesian theory for making necessary inferences that will enable for determining states of the system variables (yes or no; low,

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

medium, and high). Thereafter, we can observe the occurrence of the current system output based on BBN and use the trend for new evidence to update the probabilities in order to determine the *propagation patterns* of new causal effects generated.

For instance, P (X=low |Y=low, Z=low, T=medium) signifies that the prospect of enterprise risk once the amounts of threat (Y), cost impact (Z), and vulnerability (T) are low, low, and medium, correspondingly. The other side of it is looking at the reverse diagnostic reasoning approach. When we know certain possibility of the enterprise risk, we will then infer the prospect of a risk factor. For instance, P (Z=medium X=high) denotes that whenever the enterprise risk level is high, the prospect of cost impact is medium.

3.4. Identifying Threats to Information Assets

The question to ask when conducting a risk analysis on how to prevent information theft is, "*What can happen to our information?*" The answers are long but broadly classified to include the following:

(i) Virus infecting server that stores the data and tries to corrupt the files
(ii) Trojan horse copying sensitive and personally identifying information's to be transmitted to an attacker's FTP site.
(iii) Staff leaving a backdoor in an application to steal or destroy information,
(iv) Employee can lose a laptop with vital information's,
(v) Denial of service (DoS) attacks can affect key database and applications.

Enterprises must protect the privacy of information irrespective of how it is stored, through the depiction of the diagram in Figure6 for the campus network sensor placements with other articulated control measures and mitigation strategies that could be put in place.

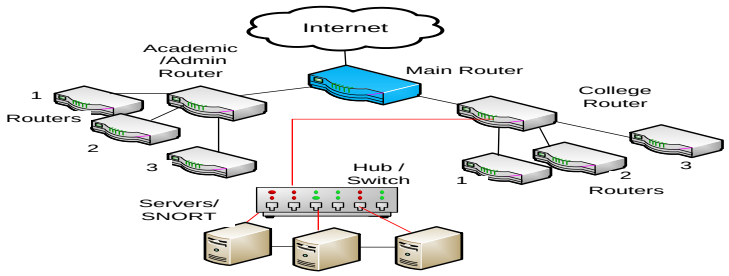


Figure6. Tools Setting for Statistical Data Collection on the Campus Network Environment

4. THE CONSEQUENCE OF NETWORK SECURITY CONTROL MEASURES

Human existence could be grand when we can all exchange information freely rather than be worried about any malicious intent, stealing or sabotaging information. However, we do not reside in a perfect

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

world, so we have to stress about the security and safety associated with a data we send across any network. Since we depend increasingly more every day on the web to handle accounts, medical records, and credit card obligations, we have to safeguard this unique information. What this means in essence is we should use network security.

The idea of network security is using the intent of creating security techniques to safeguard most valued assets in the ongoing threat of cyber crooks. When mentioning network security, we are seriously concerned about the three-dimensional solution composed of hardware, software and physical security techniques accustomed to combating any security threat. The network products like hubs, IDS's and fire walls are hardware products used inside a network to provide security to all its customers. Anti-virus software and VPN's are programs that add more protection for any network. Probably the most secure systems are the mixture of hardware, software and physical security techniques together, providing the most effective protection to any or all customers associated with the network[14].

Let us take a look at a couple of some common tools employed to secure modern network systems.

Firewall is probably the most fundamental and simply implemented techniques for network security. A firewall could be software based such is exactly what we have for windows system, or hardware based, like a router. The fundamental idea behind a firewall would be to allow approved access to a computer while obstructing unauthorized access. This is achieved by setting up access conditions according to user defined rules or policies, IP addresses, and port ease of access.

VPN is utilized to establish an encoded connection across a network when using the Internet as a transmission medium. The advantage for this is two-folded. First, it is affordable. Rather than setting up additional equipment and services to produce a secure link between one place and the other, a VPN uses the website that is already in position. The second is it helps in having a safe and secure data connection on the net. VPN connection software encrypts the information sent between one place and the other. This is what is referred to as tunneling. It receives this tag as a result of its action of tunneling computer data online while encapsulated within an encryption channel.

Intrusion Detection Systems contain a mixture of both software and hardware and work along with firewall. IDS models utilized to identify an invasion threat to some computer. IDS designs use data analysis algorithms to check data packet construction and frequency to established packet content definitions. When the packet construction is observed and does not match the expected packet construction, when compared with the previous configuration definitions, an alert in the form of reminder is signified. With respect to the configuration from IDS, the observed traffics are blocked or let the right through and marked for observation later on.

Modern computer security is dependent on the removal of known threats. Whenever a security flaw is located, it is patched. Whenever a virus is seen, it is cataloged by security companies to ensure that it can be detected and removed. Whenever a Trojan viruses rears its mind, it is quickly dissected. The researchers are normally companies, institutions and government authorities around the world spending so much time to discover defects and uncover infections, and when uncovered, solutions provided and distributed. However, with a zero-day threat, it is not possible since the malware utilizes a security flaw which was formerly unknown. As a result, the malware and /or spyware have the capacity to propagate freely until it draws the attention of security researchers. Any malware that infects personal computer may attempt to handle a number of tasks generally known as its payload, on the computer. The payload may be developing a backdoor that may later be employed to dominate the computer, or it may be to attack certain files, or it could use a keylogger. A variety of malware uses these payloads, including

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

zero-day threats. Normal malware threats and zero-day threats vary because the latter utilizes a formerly unknown flaw to spread. What this means is that zero-day threat can spread uninhibited; however, it does not always mean the outcome from the threat is much more severe than known malware.

4.1. The worm defense strategies

The possible means and ways that could be employed in order to curtail the excess of the prevailing propagation of malware on the network environment typically categorized based on the underlying strategic factors[15]:

(i) Deployment implementation strategy- Host implementation and Network through router implementation entities (thus patching through the host is more efficient than router).

(ii) The adaptation of defense strategies, either active or passive worm defense. This is through proactive and active implementations.

(iii) Destination of the worm defense system through protection or containment. By adopting the strategy that best fit the organizational policies on protection or containment.

(iv) The type of treatment response based on detection and adaptation of the worm defense strategies. Thus, detection could be signature, abnormal Net flow and abnormal behaviors.

The concepts of security self-defending networks provide for the professional networking experts to understand the methods of deploying an end – to – end, integrated network security solution. The procedure provides a clear view of all the enabling components to achieve the design and monitoring. It also makes the network to be more proactive in preventing and mitigating against any possible attacks.

Network attacks: the network has the following as the main categories of attacks-(i) Virus, (ii) Worm, (iii) Trojan horse, (iv) Denial of service (DoS), (v) Distributed denial of service (DDoS), (vi) Spyware, and (vii) Phishing.

In the same vein, there are also some traditional ways that could be employed to provide the network defenses such as- (i) Router access lists (ACL), (ii) Firewalls, (iii) Intrusion Detection / or prevention Systems (IDS / IPS), (iv) Virtual Private Networks (VPNs), (v) Antivirus programs, and (vi) Patch management.

The distinction between self-defending and traditional network defenses is that, self-defending networks has the ability to provide automatic protection of the network components and the end-user workstations during a network attack as against the traditional defense. Since the layered self-defending network have specific components that protect all the network connections that are in the data center; all branch and remote locations. Defense-in-depth strategies [16] are employed for implementing a multiple layered defense system for combating multiple security issues. The Figure 7 illustrates the common use of multiple layered form of defense in order to curtail against effects of vulnerabilities based on typical factor of Denial of Service.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

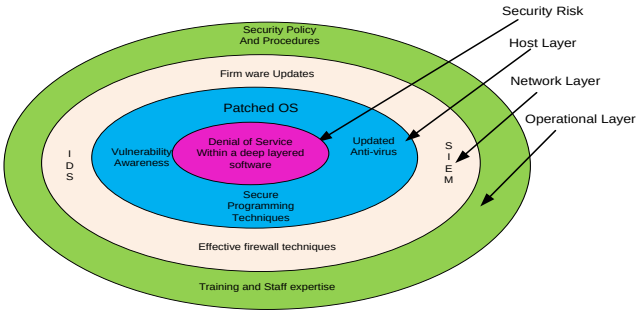


Figure7. A layered defense for protection against system vulnerabilities like Denial of Service (DoS)

The layered defense strategy based on the application of appropriate security countermeasures across the system operation, network, and host functionality. Aggregating the security activities will provide the desired protection over the entire network architecture.

Internet Connectivity means the chances that an end user is infected based on its link to a malicious server on the internet. This entails that the number of servers on the network that is compromised are a ratio of those that are not to give the probability of connectivity. Thus connected to a malicious server is $= \frac{C_m}{C_m + C_n}$ (10) Where m and n stand for malicious and non-malicious servers. If not connected to a malicious server, the ratio is $1 - \frac{C_m}{C_m + C_n}$. This is as in Figure 8.

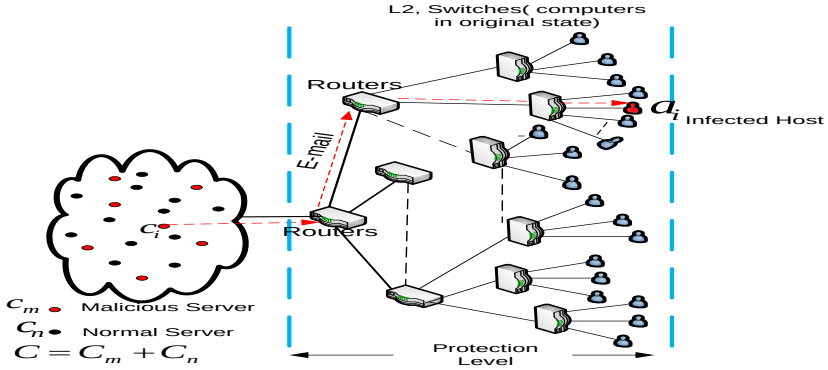


Figure8.Internet Enterprise Connectivity

The characteristic of control entity based on the availability of the measure in place. For instance anti-virus software, the fact that it is available and applied for the desired control measure, its probability of occurrence based on it put in place. Thus, luck of it in place will be an indicator of no control. Meanwhile, risk event is a factor that is determined based on the effectiveness of any available control measure in an event of visiting any malicious server on the internet. This final consequence will be as a result of the compromised effect on the asset that leads to information loss or data stealing from the enterprise network. This scenario is depicted in the Bayesian Belief Network of Figure8.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

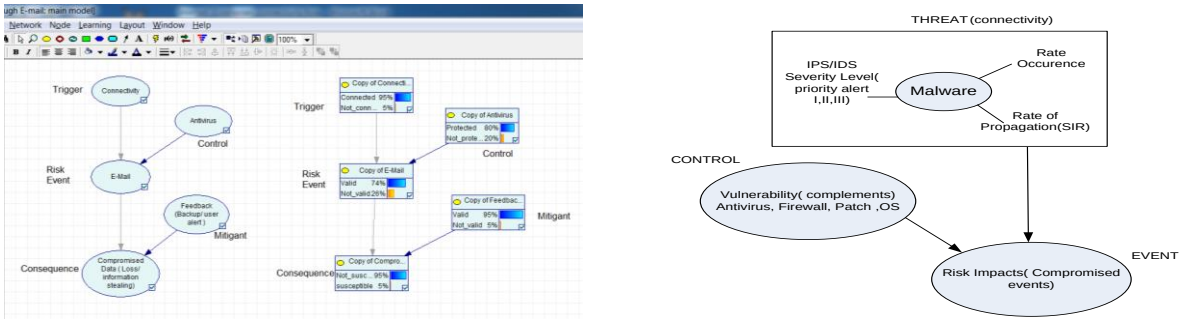


Figure 9 Connectivity through e-mail

4.2. The Sniffing Control Characteristics with IDS Sensor

Based on the security process control structure pointed out, the attack and defense actions in the diagram of Figure10 are referred to through the following numbered actions*[17]:*

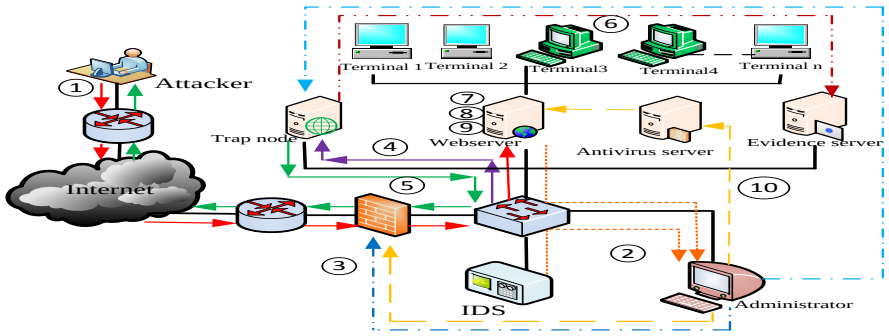


Figure10 Control Action Characteristics of an Enterprise Network [adapted from Yuanzhuo Wang et.al]

(1) Scan the weak ports from the target web server and evaluate the net service supplied by the prospective target and also the operation system from the target.
(2) IDS identify the attack and send information to the administrator server.
(3) The administrator server orders the firewall and trap node to induce the attacker to go into the trap node.
(4) The attacker makes its way into the trap node.
(5) The trap node returns the false information towards the attacker.
(6) The trap node and also the evidence server work collaboratively to get the proof of the attacker.
(7) The attacker cracks a typical user's user name and password via a weak spot from the Web server after which grants permission to itself.
(8) The attacker will get the capability root by going through the database.
(9) The attacker installs the sniffer within the Web server while using root privilege and will get the key data on the internet server and also the devices.
(10) The administrator server orders the firewall and anti-virus server to blockade the IP from

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

the attacker and take away the sniffer.

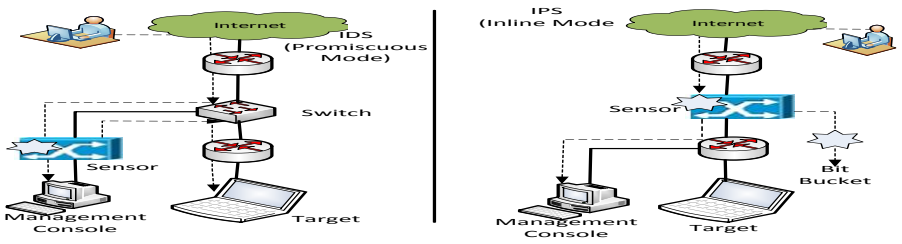


Figure11. The IDS and IPS Operational Differences

The operational differences of IDS and IPS are typically based on their placement on the network as indicated from figure 11. IDS are mostly placed in a promiscuous mode such that it allows the attacker to get to the target but could only register an alert for the occurrence of compromise with possible severity level. On the other hand, IPS is placed in an inline mode to see the attacker and stop the consequence from reaching the target. At the same time, IPS has the ability to prevent the compromise from taking place through strong control mechanism.

4.3. Client Server Connectivity Control

The effect of the placement of sensors on the network is to provide the infection alerts as a result of the malware propagation on the enterprise infrastructure network. The client server interaction protection is carried out on the network through both distributed and centralized control system. The connectivity probability due to malicious and non-malicious servers on the client visiting links at prescribed period of time through the sensor alerts. In Figure12, it shows the interaction of client **i** with malicious server on the network.

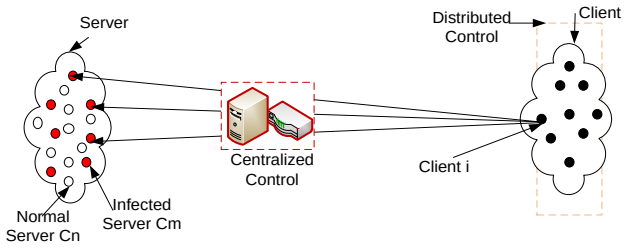


Figure12. Client Server Connectivity

The probability for client i connecting to the malicious server at time t_k is = $\frac{C_{mi}}{C_{mi}+C_{ni}}$ (11)

At time t_t , assuming there are j numbers of clients, the probability of connecting to a malicious server at time t_t = $\frac{1}{j}\sum_{i=1}^{j}\frac{C_{mi}}{C_{mi}+C_{ni}}$ = $\frac{1}{j}\left\{\frac{C_{m1}}{C_{m1}+C_{n1}}+\frac{C_{m2}}{C_{m2}+C_{n2}}+\ldots\ldots\ldots+\frac{C_{mj}}{C_{mj}+C_{nj}}\right\}$ (12)

Given that C_{mi} and C_{ni} are the connected pairs (clients and servers) at time t_t. The pairs are obtained either through net flow information Snort filtrations results / logs, and others.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

Availability of control does not necessarily mean effectiveness of control. An anti-virus solution can exist, but if the signature is not updated or the signature does not contain the pattern to detect the virus, then it becomes ineffective. Thus, the measure of availability is the measure of effectiveness. In the case of virus infection through e-mail, control can be done by applying antivirus at the gateway and host-based anti-virus. A typical example, if the user is using yahoo mail, gmail etc, the provider will scan the mail (attachment) before the downloading takes place to the sender. Similarly, in an enterprise environment, the e-mail gateway will have the facility of anti-virus protection. Similar protection is also available at the host-based anti-virus making a nest of controls.

4.4 Consequence determination through alerting sensors and connectivity

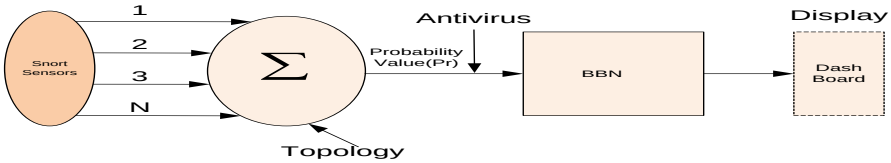


Figure13. The rate of infection intensity and the sensor aggregation procedure.

The diagram in Figure13 shows a typical communication between infected hosts with neighboring hosts. This is determined through the aggregation process depicted in Figure 13 and propagated through Genie tool of Figure 16.

	Time	Source	Destination	Protocol	Info
2049	-68.390625	00:00:00_00:00:00	00:00:00_00:00:00	0x1984	Netmon Train
168	0.468750	172.16.0.93	Broadcast	ARP	who has 172.16.1.60?
209	0.687500	172.16.0.29	Broadcast	ARP	who has 172.16.1.75?
217	0.781250	172.16.0.9	Broadcast	ARP	who has 172.16.0.94?
218	0.796875	172.16.0.9	Broadcast	ARP	who has 172.16.0.95?
229	0.859375	172.16.0.9	Broadcast	ARP	who has 172.16.0.96?
256	0.937500	172.16.0.9	Broadcast	ARP	who has 172.16.0.97?
282	1.000000	172.16.0.9	Broadcast	ARP	who has 172.16.0.98?
283	1.015625	172.16.0.9	Broadcast	ARP	who has 172.16.0.99?
317	1.093750	172.16.0.9	Broadcast	ARP	who has 172.16.0.101?
328	1.109375	172.16.0.9	Broadcast	ARP	who has 172.16.0.102?
364	1.140625	172.16.0.9	Broadcast	ARP	who has 172.16.0.103?
378	1.156250	172.16.0.9	Broadcast	ARP	who has 172.16.0.104?
389	1.171875	172.16.0.93	Broadcast	ARP	who has 172.16.1.55?
476	1.250000	172.16.0.9	Broadcast	ARP	who has 172.16.0.105?

Figure14. Malicious hosts propagation

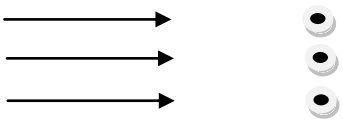
Taking the source host 172.16.0.9 as an example and in this snapshot the destinations hosts are 172.16.0.94 to 172.16.0.104 in Figure 14. The difference here would be the time difference between consecutive contacts of infected hosts to the neighboring hosts. In this case, the destination hosts can be either immune hosts, susceptible hosts or other infected hosts.

Table1. Infection rate determination

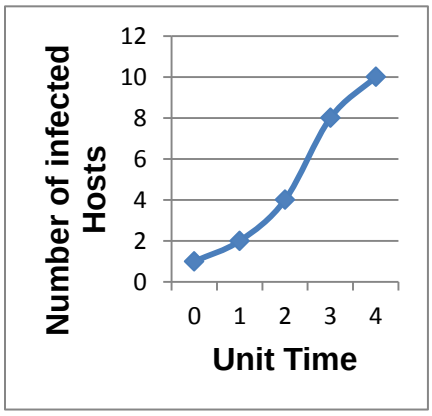
Absolute time (secs)	**Difference**	Infected host (starting time)	Propagation time	Destination Host
0.78125		0.78125	→	
0.796875	0.015625	0.796875	→	
0.859375	0.0625	0.859375	→	

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

0.9375	0.078125	0.9375
1	0.0625	1
1.015625	0.015625	1.015625
1.09375	0.078125	
1.109375	0.015625	
1.140625	0.03125	
1.15625	0.015625	



The average difference is 0.041666667s and the median is 0.03125 as shown in Table1. The actual contact time would be the starting time of the packet traversing the network path from source to destination host plus the propagation time. Even if the distance between hosts is 1 km apart, the propagation time is $1/(3 \times 10^5)$ i.e. 3.3 µs which is very much less than the average time of each initiation of infected packet transmission. Thus, the average contact time can be taken as the average time between infected packet transmissions. Here, we can assume **β** to be 0.041666667sec. This implies that every infected host will infect neighboring host at the rate of 0.041666667sec for each susceptible host. If there are 8 susceptible hosts, then the total time to infect is 0.041666667s x 8 i.e. after 0.333333336s, all 8 susceptible hosts will be infected. The smaller the value of β, the rate of infection will be faster. In the ideal case, the infected hosts grow exponentially following a geometric progression, 2^0, 2^1,2^2, 2^3, …., 2^n with interval β. An example of an exponential graph and the infection rate are as shown in the figures below:



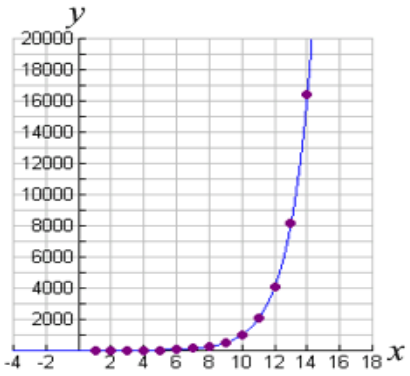


Figure 15(a). Propagation Rate per unit time Figure 15(b) C. Exponential propagation rate

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

In reality, a more probabilistic approach has to be taken since within each interval, there will be hosts which are immune and hosts which are already infected.

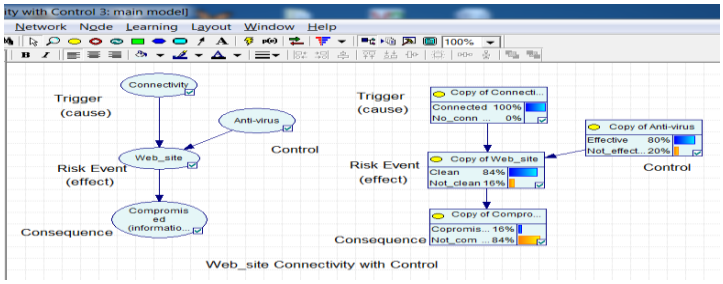


Figure16. Web site connectivity with Antivirus

Using the propagation rate as the connectivity factor on the network, we will be able to observer the effect of the malware infection and the consequences posed through the Bayesian Belief system. This is propagated by the tool Genie and depicted in Figure 16. It shows that the smaller the infection rate the faster the propagation and the higher the connectivity ratio on the network.

5. CONCLUSION

Threat analysis methods provide effective ways of differentiating between what are actual and perceived risk on the network. Therefore, risk evaluation is a kind of challengeable task and is truly a long term issue to enable for the running of robust campus networks infrastructure. The evaluation result goes a long way in helping the management to improve on the levels of information security system of the organization. Clear understanding of malware and virus and their associated propagation mechanism structure that forms the attacks channels is a critical part in recognizing how to protect against the overall threats and risks on the campus network environment. The security network management system based on Bayesian Belief decision support system provides a clear understanding ability to inform for management policy implementation and pave way for a better decision making.

We have shown through analysis the ability to have a comparable concept of malware prevalence and impact through Bayesian Belief Network inference decision systems. The inference engines overall importance in measuring and understanding of threats and information security risk management as a view point of enterprise and academic computing environment. These consequences provide the enabling ground for effective control and mitigation strategies to be in place. With the clear concept, it will provide for a trust in the expected levels of security to ascertain whether organizational security investments paid off or not through a measure based on belief network inference decision. As an on-going research activity, is expected that we will extend the inference analysis with the campus network assets assessment results through a comprehensive network security decision framework. The framework is aimed at providing an enabling ground for effective control and safeguards of the infrastructural assets on the network.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

6. References

[1] K. Liyakasa, "Cracking the Code on cyber crimes," www.detinationCRM.com 2012.

[2] N. Fenton and M. Neil, "The use of Bayes and causal modelling in decision making, uncertainty and risk " 2011.

[3] P. Weber, *et al.*, "Overview on Bayesian networks applications for dependability,risk analysis and maintenance areas," *Elsevier -Engineering Applications of Artificial Intelligence,* 2012.

[4] S. Kondakci, "A Composite Network Security Assessment," *The Fourth International Conference on Information Assurance and Security,IEEE,* 2008.

[5] R. Bernard, "Information Lifecycle Security Risk Assessment: A tool for closing security gaps," *Science Direct- Computers and Security,* 2007.

[6] M. Li. And C. Chi., "Decision analysis of statistically detecting distributed denial-of-service flooding attacks," *International Journal of Information Technology & Decision Making,* vol. Vol. 2, No. 3, 2003.

[7] A. Josang, "Conditional Reasoning with Subjective Logic," *Journal of Multiple-Valued Logic and Soft Computing* vol. 15(1), pp. pp. 5-38, 2008

[8] R. C. Stalnaker, "A theory of Conditionals," 1970.

[9] G. Yap, *et al.*, "Explaining Inferences in Bayesian Networks," 2007.

[10] J. Pearl, " Probabilistic reasoning in intelligent systems " *Morgan Kaufmann, San Mateo, CA,*, 1988.

[11] D. Heckerman, "Bayesian Networks for Data Mining," *Data Mining and Knowledge Discovery,* 1997.

[12] A. Janjic, *et al.*, "A Practical Inference Engine for Risk Assessment of Power Systems based on Hybrid Fuzzy Influence Diagrams," *Latest Advances in Information Science, Circuits and Systems,* 2011.

[13] Decision Systems Laboratory, *et al.*, "GeNIe," 2007.

[14] G. Tahan, *et al.*, "Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features," *Journal of Machine Learning Research,* pp. 949 - 979, 2012.

[15] Liuqi and M. Guoqing, "The Research and Development of Worm Defense Strategies," *IEEE,* 2010.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095

[16] "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," National Cyber Security Division 2009.

[17] Y. Wang, *et al.*, "Modeling and security analysis of enterprise network using attack–defense stochastic game Petri nets," *Security and Communication Networks, Published online in Wiley Library*, 2012.

* Corresponding Author: Address: Faculty of Electrical Engineering, Department of Microelectronic and Computer Engineering, Skudai, Johor, 81310 Malaysia, aliyubiu@gamail.com, +60146109095