A MODEL FOR CYBER ATTACK RISKS IN TELEMETRY NETWORKS

Neda Bazyar Shourabi
nebaz1@morgan.edu
Advisors: Drs Richard Dean, Farzad Moazzami and Yacob Astatke
richard.dean@morgan.edu
farzad.moazzami@morgan.edu
yacob.astatke@morgan.edu

ABSTRACT

This paper develops a method for analyzing, modeling and simulating cyber threats in a networked telemetry environment as part of a risk management model. The paper includes an approach for incorporating a Monte Carlo computer simulation of this modeling with sample results.

Keywords: Risk Management, Cyber-attack and Monte Carlo simulation

1 INTRODUCTION

It is difficult to overstate the risks of cyber security attacks on government and business interests of this country. Reports of hacker break-ins at major institutions appear in the media every day [1]. Technical and management resources are pouring into this problem but there is little hope of a strategic solution in the foreseeable future. Experts in the field have come to realize that some technical "silver bullet" will not emerge. Rather, there is an increasing need to manage the residual risk of IT networks. Figure 1 illustrates this dilemma. The Venn diagram shows the space of current vulnerabilities in IT networks along with the space of known defenses. It is well understood that the state of both the vulnerabilities and the defenses are changing with time.

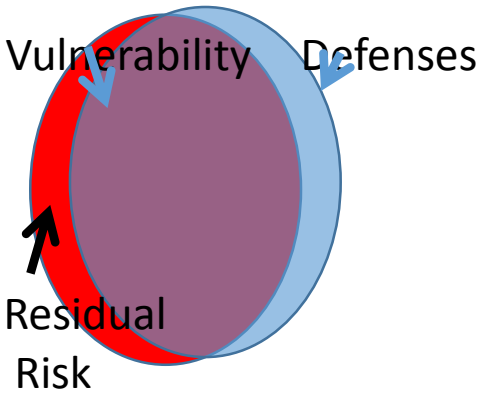

Figure 1: The Risk Space

Good defense solutions are available for most well documented attacks of the past. New or recently developed attacks such as Day Zero attacks [1] represent a continuing risk to well managed IT systems. This points to the need for management of residual risk. NIST guidelines on Risk management represent some of the best strategies for doing this. These models do not however provide quantitative measures by which enterprises can assess, plan, or manage risk. This paper shows a model that has the potential to address these issues.

2 CYBER SECURITY RISK MODELS

The complexity of risk management requires a variety of tools and models necessary to support technical and risk decisions for an IT network. Three such models are presented here which include Process Models, Analytical Models and Simulations.

Process Models [2, 3] as developed by ICASA and NIST are needed for enterprises to organize and develop risk strategies. Such models script the activities and events needed to assess, plan and manage risk.

Analytical Models abstract the response of the IT network to attacks and develop analytical measures that would forecast the behavior of networks based on mathematical representations of the system behavior.

Simulations are analytical models that have been transformed into functioning modules that can be adapted to represent a wide variety of possible scenarios with results that can be observed and analyzed.

All three of these models are needed for risk analysis but the Process Model is the only validated and widely available model. This paper develops the analytical model for an IT system under attack and shows the results of simulations that reflect the analytical model. The value of these models is potentially significant. Such models allow the enterprise owners the opportunity to model their systems and create "what-if" scenarios. These evaluations might illuminate current risks in the system, enable an investment strategy for reducing the risk posture of the enterprise, or develop performance measures that would drive risk to acceptable levels.

3 GENERAL FRAMEWORK

A general model for the cyber risk of an IT network has been developed as shown in figure 2. This model follows from NIST [4] and others.

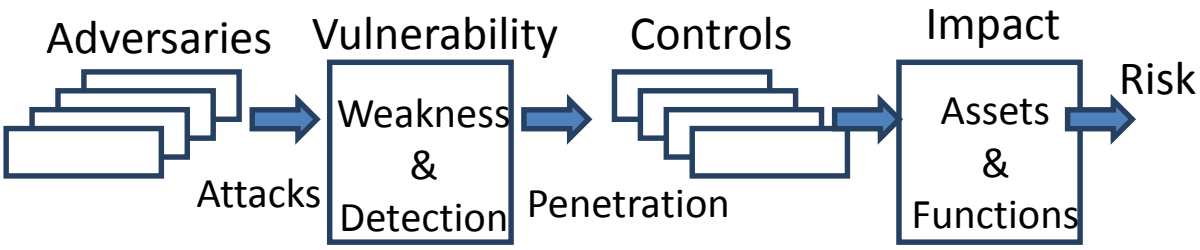

Figure 2: Risk Model for a Cyber System

Adversaries launch multiple attacks against a target network which have a set of known or potential vulnerabilities. A subset of these attacks are detected and removed while others are successful in penetrating the system to achieve harm to the enterprise. A layer of controls are available to manage and remove these penetrated attacks. A residual of effects are applied against the assets and functions of the enterprise which results in risk. Risk is the expected cost associated with operating your system in the presence of attacks. Risk costs can be tangible (loss of business) and express in dollars, or intangible (loss of reputation) which can also be translated into dollars. Much of today's emphasis in cyber risk management is related to reduction of vulnerability with technologies such as firewalls, virus scanners, and intrusion detection systems shown here as weaknesses and detection. Less attention is paid to the controls in a cyber-system which includes technology but also policies and practices that address the removal of the attack and the recovery

of the system. Both the vulnerability and the controls components in this model have response times for dealing with attacks and penetration which are critical to the overall reduction of risk. These elements are captured in an analytical model as parameters in a stochastic system which drives the risk of the enterprise.

4 MODEL ELEMENTS

Attack Model:

The attack model can be modeled as a random process of arrival with a Poisson probability density function (pdf). This function is commonly used for a variety of arrival applications including cyber attacks. The probability of k occurrences of attack (i) during any specified interval of time can be expressed as:

$$Pa(k) = \lambda i^{k} e^{\lambda i} / k! \quad (1)$$

Where λi is the average arrival rate of k attacks (i) and k = 0, 1, 2, 3… ∞ in some interval T.

The probability that an attack is present, PA, can be expressed as the probability of one or more attacks

$$PA = \sum_{k=1}^{\infty} Pa(k) \quad (2)$$

Vulnerability:

The success of an attack depends on the presence of a vulnerability and the ability to avoid detection. Assuming a vulnerability is present, success then depends on the ability of a detection mechanism to deter the attack. This depends on the time available to for detection. An exponential pdf is a good fit here where

$$Pd = \lambda_2 \ e^{-\lambda 2} \quad (3)$$

Whereλ_2 represents the average time for detection, and the conditional probability of a successful Psa attack in time T is:

$$Psa/attack = 1 - e^{-\lambda 2 T} \quad (4)$$

If the attack is detected or the time to detect is small, Psa is near zero, whereas, if the Time to detect is large, Psa approaches 1. This is applied to each of the attacks (i). The model assumes that some subset of attacks are successful over time and have penetrated the system.

Controls:

Security controls represent an independent mechanism which addresses the management of the system in the presence of penetrations. These are a second layer of defenses that protect the system in the presence of a penetration. These include technology components such as software integrity tests, as well as policies and practices, such as the reporting and review of anomalous behavior by security managers. While these penetrations and controls are different, they can be modeled in a fashion similar to attack detection shown above. The success of a penetration depends on the time it takes for security controls to detect and remove a penetration. The exponential pdf is a good choice to model this as is reflects success probabilities over a wide range of times for as:

$$Ppd = \lambda_3 \ e^{-\lambda 3T} \quad (5)$$

Where λ_3 represents the average time it takes to control a penetration and the probability of success of the penetration at time T is

$$Psp = 1 - e^{-\lambda 3T} \quad (6)$$

This reflects a zero probability if the penetration is controlled immediately and a probability that approaches 1 as time grow larger.

Impact:

The impact of a successful penetration may lead to several effects. Tangible and intangible assets are at risk. Penetration in to a banking system might lead to the direct loss of money. The hack into the Target Corp had intangible effects, the loss of personal information and credit card data. While intangible, these effects cost Target hundreds of millions of dollars due to reputation loss. For the purpose of this model it is assumed that the impact of the penetration is tangible loss limited by the net worth ($NW) of the enterprise. The extent of the loss for an attack (i) is assumed to be proportional to the total penetration time Tp which exponentially approaches the $NW as:

$$Loss_i(T) = (1 - e^{-\lambda 4Tp})\$NW \quad (7)$$

Where λ_4 represents the time constant for dissipation of assets from the enterprise.

Risk:

Risk can be measured as an aggregation of costs and their associated probabilities. In a multi-attack environment the aggregate risk can be expressed as:

$$Risk = \sum_i Psp(i)\ Loss_i\ (T) \quad (8)$$

This can be express from equations 1, 2, 4,6 and 7 above as

$$\text{Risk} = \sum_i \left(\sum_i \left(\lambda_i^k e^{\lambda_i}/k!\right)\right)\left(1 - e^{-\lambda 2T}\right)\left(1 - e^{-\lambda 3T}\right)\left(1 - e^{-\lambda 4Tp}\right)\$NW \quad (9)$$

This expression depends on an ability to estimate the parameters associated with each element of the model. In a real enterprise much of this data can be estimated from detection and monitoring devices in the enterprise. Simplifying assumptions might be necessary to get numerical results. This expression has value in that the λ values and the time constants represent risk performance measures and your management can drive or monitor your enterprise risk with these values.

5 SIMULATION

A Matlab Monte Carlo simulation was accomplished and tested for several scenarios. The experiments were directed at comparing risk as a function of the emphasis on the detection versus control in the system. For simplicity a single attack type was assumed. With the λi fixed for attack arrival and cost, the λ2 and λ3 are varied for 4 different strategies:

- Small emphasis (10%) on both detection (λ2) and control(λ3)
- High emphasis (50%) on detection only
- High emphasis (50%) on control only
- Balanced emphasis (35%) each on detection and control

These experiments presumed that the emphasis on any feature was driven by limited resources and, that improvement saturated at some point. Emphasis was increased by increasing the values of λ2 and/or λ3.

Figures 3,4,5,6 each show plots of attacks, detections, penetrations, controls and cost consequences with the different strategies. Note the first subplot shows events that correspond to the presence of an attack on the system. The second subplot shows a subset of successful detection/removal for a corresponding attack. The third subplot shows the residual attacks that penetrate the system and the fourth subplot shows a subset of controls that remove a corresponding penetration. Finally the fifth subplot shows an accumulating cost associated with each successful penetration with an accumulated risk of .4 normalized to $NW.

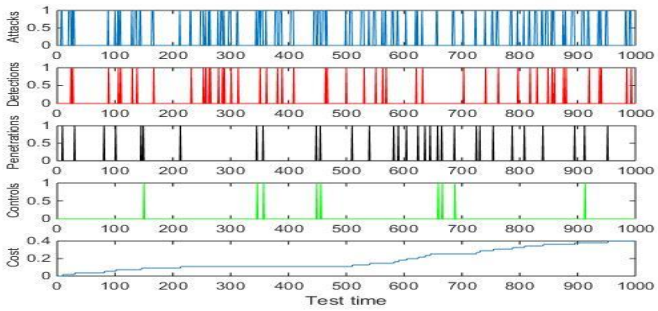

Figure 3: Case one, No Emphasis

The second experiment provided an enhanced emphasis on detection. In Figure 4 one can see the dramatic reduction in penetrations when detection efficiency is improved. Note that the accumulated risk falls to about .2.

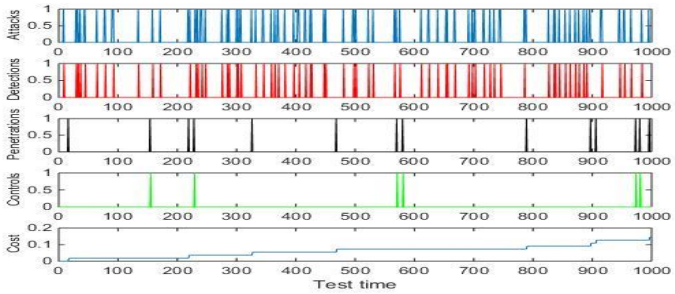

Figure 4: Case two, Emphasize Detection

In case 3 the experiment was varied to add emphasis on the Control element only. Figure 5 shows a significant improvement in the penetrations that are removed in the system with an accumulated cost of about .2.

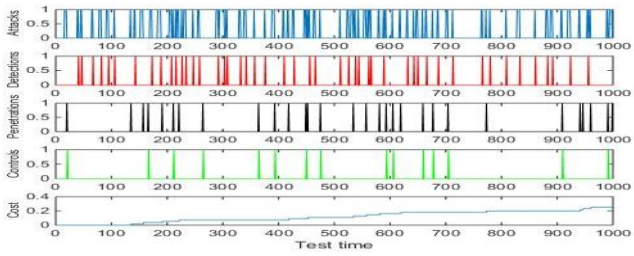

Figure 5: Case three: Emphasis on Control

The final experiment was a balanced improvement on both detection and control features. Figure 5 shows improved removal of attacks in both the detection and control elements of the simulation with an aggregate risk of about .08.

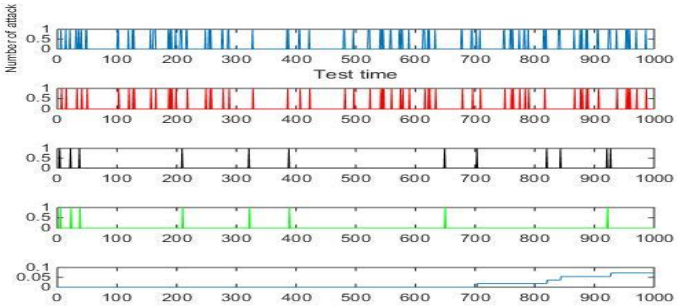

Figure 6: Case four: Balanced Emphasis on Detection and Control

Comparing the results of the risk (cost) of the four experiments is instructive, Figure 7 depicts the cost for each trail with the different strategies. It is clear that the balanced approach to detection and control is the lowest risk and most effective strategy. This confirms what many security experts predict in the risk management of systems. It also suggests that this model could be successfully expanded to a variety of other experiments to assess different strategies for risk management.

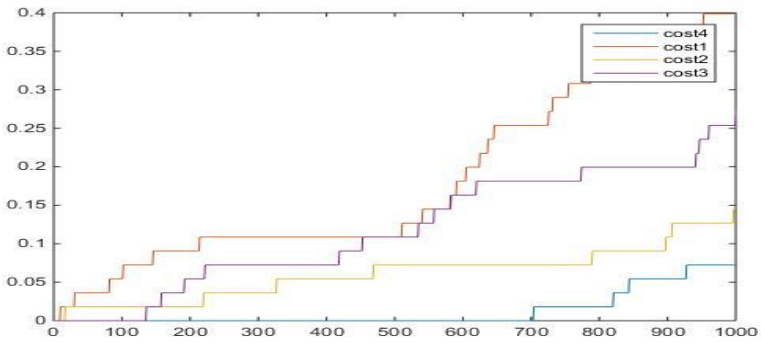

Figure 7: Comparing cost for all four cases

6 ANALYSIS

Adversaries can penetrate a system when the system either doesn't recognize the attack or is unable to control it. In case one, as figure 3 shows, between time 0 and 100 there are several attacks but because the system detected just some of them, the remainder penetrate the system and few controls are effective, and so the costs are shown to increase.

In case two, as in figure 4, we emphasize detection. Notice that the detection of attacks are significantly increased. However several attacks still penetrate, and with weaker controls the cost increases buts is less than in case one. In case three, as shown in figure 5, we add an emphasis on control. Note that between times 600 -700, there are numerous attacks and the detection is limited and therefore we have numerous penetrations. In this case the controls are enhanced and many of the penetrations are reduced with an overall reduction in cost compared to case one.

In case 4, as shown in figure 6, we balance the emphasis on both detection and control which achieve the overall best results. Note that in the timeframe 0-700 there are no successful attacks and the cost is zero. In the timeframe 700-800, there is just one successful attack with minimal cost. Finally in timeframe 800-1000 there are four successful attacks but with an overall cost much better than cases one, two and three.

As noted early in this paper changing emphasis on cyber control or detection has to be considered. We demonstrate that the balanced emphasis between detection and control elements in the system provide the best overall performance. The paper showed how, by analysis and simulation, risk could be managed to reach the lowest cost.

7 CONCLUSION

Future networked telemetry systems will require significant attention to cyber security attacks and risk assessments that are part of their deployment. A framework for Risk management is demonstrated which points to three models for assessing, planning, and managing risk. While good process models exist, analytical models and simulations do not. An analytical model for Risk is developed and a simulation of that model is presented. Results from the risk simulation are presented. These results show how parameters in the simulation that characterize the probabilities in the model can be varied to assess risk in a network. The specific example showed experiments

where emphasis was placed alternately on detection of attacks and the control of attacks. The results show that a balanced approach to these features results in the lowest risk. This agrees with the prevailing wisdom on the cyber security community and points to the potential of these tools to be developed and used for future cyber security risk management.

8 FUTURE WORK

This paper presented a framework for managing risk based on analytical models and simulations. While results presented are encouraging, there are a host of simplifying assumptions made to accomplish this work. The probability distributions and parameters were assumed and these features need verification. There is a wealth of data on attacks that are published and it is expected that this would be tedious but straightforward. There would also need to be parameters which would characterize future new attacks. The parameters and results of this model should also be mapped into some real networks to demonstrate that the behavior and the estimated risks are sufficiently reliable.

REFERENCES

[1]P. Passeri, Cyber Attack Statistics, http://www.hackmageddon.com /category/security/cyber-attacks-statistics/, May2015.

[2] ICASA, The Risk IT Framework, Rolling Meadow, IL, May 2009.

[3]NIST Special Publication 800-39 – Managing Information Security Risk -Organization, Mission, and Information System View, March 2011.

[4] NIST Special Publication 800-30 R1, Guide for Conducting Risk Assessments, Sept 2012.