Cyber Security Quantification Model

M. Asif Khan, M. Hussain

***Abstract*—Security of information systems is a major concern today because the existing threats are getting new dimensions. Information Security (IS) is to protect our important information assets from accidental or deliberate damages. Cyber Security (CS) is a whole set of procedures and systems providing protection of computer systems and networks from the intentional and unintentional damages or dangers in the cyberspace through services like confidentiality, integrity, authentication, availability, non-repudiation, auditing, and digital signature. To counter the increasing cyber terrorism threats, we need predictive calculation of cyber attacks occurrences. We can do this by giving mathematical models for the elements of CS systems. Researchers have suggested some models for the quantification of CS, however, the existing models have either enforced only qualitative measures or the quantification models lack modeling features and without validation with the realistic data. There is a requirement for a unified model for the quantification of CS that considers majority of the parameters and services for it and which should be validated with realistic data. We propose a quantification model of cyber security, which considers most of the CS parameters. This is a generalized model, which is customizable enough to be used in multitude implementation environments. The proposed model is simulated and validated with an example of real life data for the SZABIST Islamabad Campus email server.**

***Index Terms*— Threats, Attacks, Cyber Security, and Quantification Model.**

I. INTRODUCTION

Our world is global village today. Every field of life has the usage of computer technologies and it is increasing continuously. The major reasons of growth in usage are getting the benefits of quick decision-making and rapid calculation power of computers. Mostly organizations are dependent on their information systems and communication technology for their routine business. When data of interest becomes information in digital form, it turns into an asset to be protected at all costs. Like any asset, these digital assets are also prone to attack any time. Protection of such an important asset for every organization is vital due to their dependence on it. Security of information systems is major concern for them today because the threats are getting new dimensions.

Some people think that only login and password is enough for their system security. Majority of the people think that installation of anti-virus on their systems is enough for their protection while most of the people completely satisfy themselves by only encryption of data. But, all of these individual techniques are not enough for information security. Information Security (IS) is to protect our important information assets from accidental or deliberate damages to it.

Cyber Security (CS) means the protection of computer systems and their networks from the intentional and unintentional damages, dangers, faults, fears, adversaries, unauthorized disclosure and all types of intrusions. We are very much vulnerable to cyber attacks on Internet and need continuous planning for this.

CS metrics were measured qualitatively and for that qualitative metrics some model exist in the world. But unfortunately there is no standard quantification model for CS. To counter the increasing cyber security threats we need predictive calculation of cyber attacks occurrences.

In the process of cyber security quantification, quantification metrics are the risks, vulnerabilities, threats, attacks, consequences and reliability [9]. Researchers have suggested a number of models for the quantification of CS but they are lacking modeling features and validation with the realistic data. There is a requirement for a unified quantification model for the prediction of CS parameters, which could be validated with realistic data.

In this paper we propose a quantification model for CS, which predicts values of CS parameters. The proposed model is simulated and validated with an example of real life ten years data of the SZABIST Islamabad Campus email server.

The remainder of the paper is organized as follows: the second section describes the related work done in this field. The third section will give some fundamental concepts. In the fourth section we will describe our proposed model. In section five some results of the model will be discussed.

II. RELATED WORK

Researchers have discussed several models for the quantification of CS. In the work done by Sheyner et al., Wang et al and Kuhl et al [1, 2, 3], they discussed network security analysis using attack graphs, their generation and simulation. The authors proposed automated attack graph generation model, implemented it in a tool and analyzed with different examples. However, their model only tackles attack

M. Asif Khan, SZABIST, Islamabad, asifk@email.com
M. Hussain, SZABIST, Islamabad, hmureed@yahoo.com

generations. Our approach is to quantify the attack parameter but we have not implemented it in a tool like theirs.

Madan et al. [4], have discussed the security attributes of intrusion tolerant systems and proposed quantification model for analysis of security attributes of intrusion tolerant systems. In their model the attacker's effort was modeled with exponential distribution. But our claim is that this variable (attacks) is discrete in nature and not continuous and we model attack with a discrete distribution.

Gordon et al. [5], have discussed about the problem of quantification of cyber and physical security in isolation and proposed a quantified model integrating cyber and physical security. In their proposed model the authors consider the physicals and cyber attacks paths.

In the work done by Zhu et al. [6], they assumed the modeling strategies of attacker's behavior and proposed a new model called Turing Assessor (TA). It is a simulation technique that is used for the system security. This was accomplished by the steps of system security property for functionality and evaluated for that. It only considers one functionality this is fairly limited.

Our approach of predictive quantification of CS parameters and an integrated CS model is inspired by the work of Schneidewind [7, 8, 9]. They have claimed that to protect from the destructive response of cyber terrorism to information world, predictive models would be required for cyber attacks estimation before they occur. In their work they have assumed specific security services. Our model considers all security services. They use continuous statistical distribution for discrete variables while our model assume discrete statistical distribution for discrete variables as the nature of events (attacks are discrete events) and not continuous.

III. BACKGROUND

In this paper, we propose quantification model of Cyber Security. Our model based on our knowledge learned from critical review of the related literature.

Cyber Security Quantification Model is the combination of four words; Cyber + Security + Quantification + Model.

Cyber is the combination of information systems and networks. Security is a set of measures and mechanisms used for protection from dangers or fear for things. Quantification is the property of things that is to be measured or expressed in numbers. A model is a conceptual representation of some real objects, processes, or systems in terms of measurable parameters.

Cyber Security is a whole set of procedures and systems providing protection of information systems and networks from intentional and unintentional damages or dangers. Quantification model is the representation of a system whose parameters can be expressed in numbers. Cyber security quantification model is the numerical representation of CS parameters.

IV. MODEL DESCRIPTION

Quantification model for Cyber Security is not as simple as to derive a mathematical equation for this and that is enough. To understand this process we need to examine the whole process, i.e. what are the activities involved, entities on what activities operated and relationships between them.

To understand and develop the CS theory numerical models are required. We describe and apply our numerical models for the CS parameters and services here.

Measurement is determined directly by evaluation of specific and discrete values while metrics are indirect comparison values derived from measurements. Metrics should be specific, measurable, attainable, repeatable and time-dependent (SMART) George et al. [10].

There should be a process to model a real world entity (system) and simulate that model for verification and validation. At first, an experimental frame is required to be set to identify inputs, outputs and their relationships. Then we have to characterize a class of candidate model for selection. Once a specific type of model has been selected then one need to estimate parametric values through it. After estimation has been done simulating the model so that its values can be validated and verified as compare to the real world data.

In our case the real world entity is the CS system with different parameters and services provided as given in "Fig. 7". Steps of simulation-model are given in "table.1". We are required to model its parameters and then simulate it. Experimental frame for our case is the SZABIST Islamabad Campus email server providing email facility to the campus people. Inputs to the system are the email transactions and outputs are the predicted values of risks, vulnerabilities, threats, attacks, consequences and reliability. For these predicted values to obtain we can use mathematical or statistical models (stochastic models). Through theses predicted values we can set our priorities.

First of all we describe the variables and their naming used in our models.

Variables defined are as follows:

t = Time at which an event occur.

$V(t)$ = Vulnerabilities for given threat at time t.

V = Total number of Vulnerabilities.

T = Threats existed at time t.

$P_V(t)$ = Probability of vulnerability for a given threat at time t.

$P_A(t)$ = Probability of an attack occurred at time t.

λ = Inter arrival rate of attacks.

n = Number of attacks occurred.

f = Failure rate.

$\mathrm{Re}l(t)$ = Reliability of a system at time t.

$C(t)$ = Consequence of the attack at time t associated with risk and vulnerability.

$P_T(t)$ = Probability of threat assumed at time t.

TABLE I
SIMULATION-MODEL PROCESS

Real World Entity	Model
• A prior Knowledge exists about it • Set goals for study behavior in a context • Set experimental frame having inputs (causes), outputs (effects) and their relationships • Characterize system within • context • Execute real experiment • Gain the experimental data • Analyze the data, i.e. validation • Documentation	• A prior Knowledge exists about it • Set goals for study behavior in a context • Set experimental frame definition having inputs (generator), outputs (transducer) and their relationships (acceptor) • Select a specific class of model and characterize the structure of model • Estimate data values • Execute virtual experiment (Simulation) • Gain the simulation data • Analyze the data, i.e. validation and verification of the model and data • Documentation • Implementation •

$P_R(t)$ = Probability of risk for a given threat at time t

A. Vulnerability Model

Our first model is vulnerability model, which predicts the vulnerability of any given system at time t. Vulnerability is the presence of faults or errors that may cause harm to a system.

If two events E and F are such that E is dependent on F then the probability of E is called conditional probability denoted by $P(E \mid F)$ and given as $P(E \mid F) = \frac{P(E \cap F)}{P(F)}$, Charles et al. [11]. So, probability of vulnerability for a given threat at time t is $P_{V|T}(t) = \frac{P_{V \cap T}(t)}{P_T(t)}$ (conditional probability) where V and T are vulnerability and threat respectively. But we know that V and T are independent, so $P_V(t) = \frac{V(t)}{V}$ (1).

B. Attack Model

Our second model is attack model, which predicts the number of attacks occurred at time t. Attack is a subjective entity whose intention is likely to cause harm. It follows the Poisson law, i.e. $P_A(t) = e^{-\lambda t} * \frac{(\lambda t)^n}{n!}$, where λ is the inter-arrival rate of attacks and n is the number of attacks occurred in time interval t. Here $n = \lambda t$ if we study an attack occurred at time t. So probability of an attack occurred at time t is

$$P_A(t) = e^{-\lambda t} * \frac{(\lambda t)^{\lambda t}}{(\lambda t)!} \quad (2).$$

Schneidewind [8] has used exponential distribution instead of Poisson. The attacks occurred at time t follow the Markov process so we use the Poisson distribution for it.

C. Reliability Model

Third model is reliability model, which gives the reliability of a system at time t. Reliability is the characteristic of goodness. If f is given as the failure rate then reliability of a system at time t is given by $\mathrm{Re}l(t) = e^{-ft}$ (3) [12].

D. Threat Model

Our fourth model is threat model, which predicts the threat at time t. Threat is an adversary that is motivated to exploit system vulnerability and cause damage. Probability of threat assumed at time t is given as $P_T(t) = P_V(t) * \mathrm{Re}l(t)$ (4).

Where $P_V(t)$ is the probability of vulnerability for a given threat at time t and $\mathrm{Re}l(t)$ is reliability of a system at time t as given in equations (1) and (3) respectively.

E. Consequence Model

Our fifth model is consequence model, which predicts the consequence of an attack occurred at time t. Consequence is the result or effect of some process. Consequence of an attack occurred at time t is given as $C(t) = \frac{P_A(t)}{P_T(t)}$ (5).

Where $P_A(t)$ is probability of an attack occurred at time t and $P_T(t)$ is probability of threat assumed at time t as given in equations (2) and (4) respectively.

F. Risk Model

Our sixth model is risk model, which predicts the risks at time t. Risk is the chance or possibility of danger or loss of any asset, digital in our case. It cannot be measured directly and correctly. We only assign relative values to it through different methods. In literature Richard et al. [13] gives the basic equation for Risk as:

*Risk = Vulnerability * Threat * Consequence.*

So probability of risk for a given threat at time t is given as

$$P_R(t) = P_V(t) * P_T(t) * C(t) \quad (6).$$

Where $P_V(t)$ is the probability of vulnerability for a given threat at time t, $P_T(t)$ is probability of threat assumed at time t and $C(t)$ is consequence of an attack occurred at time t as given in equations (1), (4) and (5) respectively. Schneidewind [8, 9] model is similar to our model but, in contrast, we use probability of threat instead of probability of attack.

For the process of Cyber Security Quantification all of the data is not available in measurable form rather we have metrics for them. Measurements or metrics for all these parameters should be identified and calculated. If we are given the value of t, V(t), λ, and f we can find the predicted values of CS parameters with the help of above seven equations.

V. DISCUSSION AND ANALYSIS

We are given the real life ten years data of the SZABIST Islamabad Campus email server as given in tables 2 and 3. We use MATLAB to plot our values and find the respective values of parameters.

TABLE II
INPUT DATA OF SZABIST EMAIL SERVER

Data	Time Index (t)	Type of attack	Vulnerability
2000	1	Denial of Service	587
2001	2	Virus	322
2002	3	Probe	271
2003	4	Account Compromise	134
2004	5	Packet Sniffer	124
2005	6	Root Compromise	62
2006	7	Trojan Horse	59
2007	8	Worm	27
2008	9	Spyware	17
2009	10	Corruption of Database	8

Inter arrival rate of attacks (λ) = 0.5, failure rate (f) = 0.2

We use the data given in our proposed models and find out some results as under.

1. As the number of vulnerabilities increases probability of risk increases i.e. probability of risk is directly proportional to the probability of vulnerability.
2. All the predicted values of parameters are directly proportional to the number of vulnerabilities.
3. Probability of threats is directly proportional to the probability of vulnerability.
4. As the maximum number of vulnerabilities is for the threat of DOS (Denial Of Service) so it has the maximum probability for vulnerability, attacks, threats and risk.
5. Consequence of a threat is inversely proportional to the probability of threats.

We also give the different plots for the calculated values of parameters.

Figure 1 gives the relation of vulnerability and attack. It shows that, as the number of vulnerability increases so does the probability of attack, i.e. the probability of attack is maximum at the maximum number of vulnerabilities (DOS attack).

Figure 2 shows the relation of vulnerability and threats. It gives that, as the probability of vulnerabilities increases so does the probability of threats increases (i.e. directly proportional).

Figure 3 shows the relation of threats and its consequence. It gives that, as the consequence value of a threat increases, its probability of threats decreases. Consequently, consequences having less threat, as more effort required for success.

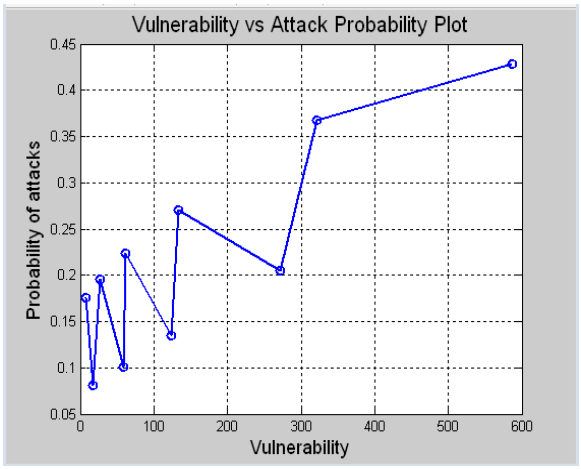

Fig.1. Vulnerability vs. Attack Probability Plot

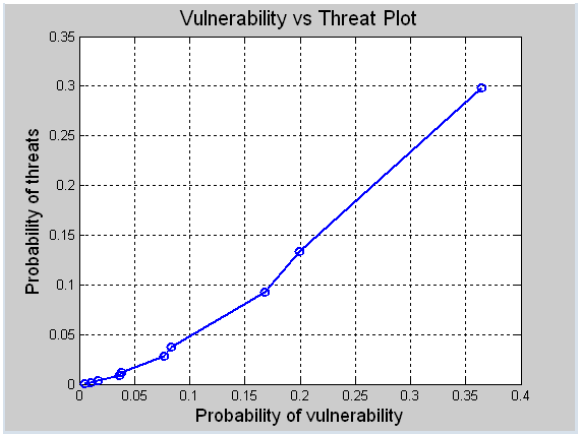

Fig.2. Vulnerability Probability vs. Threat Probability

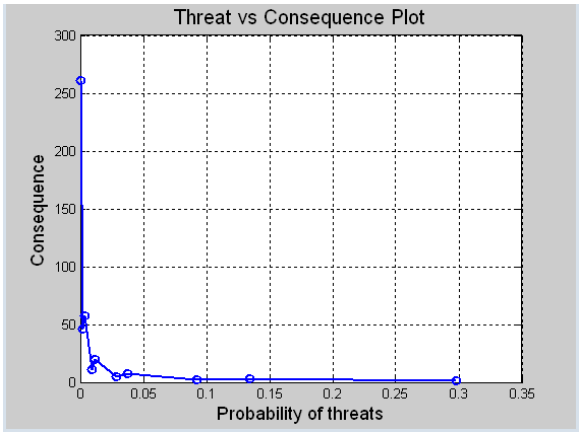

Fig.3. Threat Probability vs. Consequence Plot

Figure 4 shows the relation of threats and attacks. It gives that, as the probability of threats increases so does the probability of attacks (i.e. maximum value for the threat and attack of DOS).

Figure 5 shows the relation of vulnerability and risks. It gives that, as the probability of vulnerabilities increases so does the probability of risks increases i.e. higher

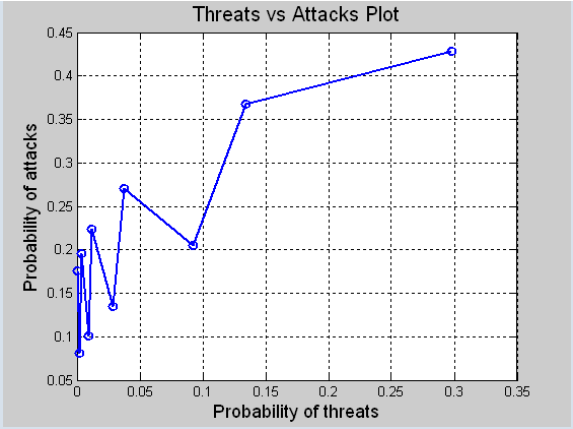

Fig.4. Threat Probability vs. Attack Probability Plot

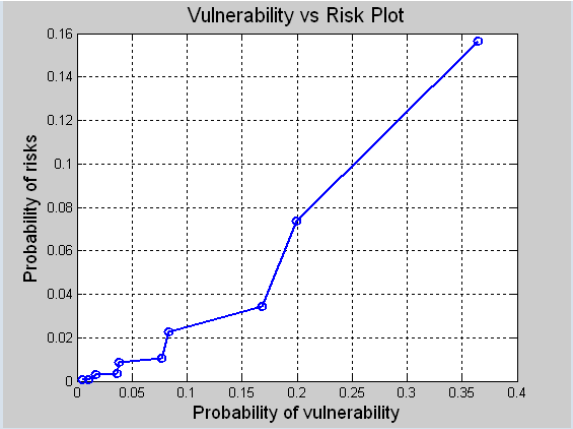

Fig.5. Vulnerability Probability vs. Risk Probability Plot

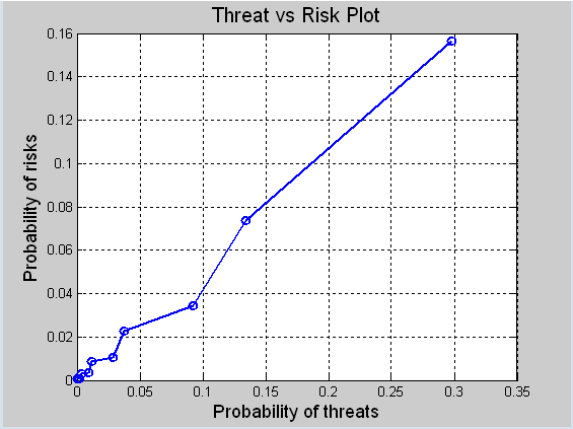

Fig.6. Threat Probability vs. Risk Probability Plot

vulnerabilities having more risks to compromise.

Figure 6 shows the relation of threats and risks. It gives that, as the probability of threats increases so does the probability of risks increases i.e. higher threats having more risks to attack.

VI. CONCLUSION

A detailed quantification model for Cyber Security is proposed that not only follows a standard modeling process and rules but also quantifies risk, vulnerability, threat, attack, consequence, and reliability. We use discrete probability distributions for discrete variables and also integrate all the parameters.

VII. FUTURE WORK

The proposed model will be implemented in an automatic tool so that a simulator could be designed. After developing an automated model, the implementation of CS and its net impact will be more easily quantifiable.

ACKNOWLEDGMENT

We would like to thank Mr. Abid Shehzad (Network Administrator, SZABIST Islamabad Campus) for provision of previous ten years data of email server attack data of the campus required for our validation.

REFERENCES

[1] O. Sheyner, J. Haines, S. Jha, R. Lippmann, J. M. Wing "Automated generation and analysis of attack graphs", *In Proceedings of the 2002 IEEE Symposium on Security and Privacy*, May 2002, pp 273-284. http://doi.ieeecomputersociety.org/10.1109/SECPRI.2002.1004377

[2] L. Wang, A. Singhal, S. Jajodia "Toward Measuring Network Security Using Attack Graphs", *Proc. of the 2007 ACM workshop on Quality of protection,* Oct 2007, pp 49-54. http://portal.acm.org/citation.cfm?id=1314273

[3] M. E. Kuhl, J. Kistner, K. Costantini, M. Sudit "Cyber attack modeling and simulation for network security analysis", *Proc. of the Winter Simulation Conference,* Dec 2007, pp 1180-1188. http://portal.acm.org/citation.cfm?id=1351749

[4] B. B. Madan, K.G. Popstojanova, K. Vaidyanathan, K. S. Trivedi "A method for modeling and quantifying the security attributes of intrusion tolerant systems", *Performance Evaluation,* vol. 56, pp. 167-186, March 2004. http://www.ee.duke.edu/~kst/security/Madan.pdf

[5] K. A. Gordon, G. D. Wyss "Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness", *Sandia Report,* SAND2005-7177, Nov 2005. http://infoserve.sandia.gov/sand_doc/2005/057177.pdf

[6] J H. Zhu, C. Chigan, F. Bao "Turing Assessor: A New Tool for Cyber Security Quantification", *Proc. of IEEE Wireless Communications and Networking Conference,* April 2006, pp. 629 – 633. http://ieeexplore.ieee.org/iel5/11060/34935/01683542.pdf?arnumber=1683542

[7] N. F. Schneidewind, "Internet Cyber Attack Model", *The R & M Engineering Journal, American Society for Quality*, 2005.

[8] N. F. Schneidewind, "Cyber Security Prediction Models", *The R & M Engineering Journal, American Society for Quality,* Dec 2005.

[9] N. F. Schneidewind, "Integrated Cyber Security Model", *The R & M Engineering Journal, American Society for Quality,* 2005.

[10] Jelen, George; "SSE-CMM Security Metrics," *NIST and CSSPAB Workshop, Washington DC, USA,* 13-14 June 2000. http://csrc.nist.gov/csspab/june13-15/jelen.pdf

[11] Charles M. Grinstead, J Laurie Snell, "Introduction to Probability" *second edition.* http://www.dartmouth.edu/~chance/teaching_aids/books_articles/probability_book/pdf.html

[12] Igor Bazovsky, Reliability Theory and Practice, *Prentice- Hall, Inc.,* 1961. http://www.amazon.com/Reliability-Theory-Practice-Dover-Mathematics/dp/0486438678

[13] Richard Enbody, "Interdisciplinary topics in Cyber Security", *Computer Science and Engineering, Michigan State University.* http://www.cse.msu.edu/~cse429/lectures06/lecture1.ppt

1999-4974©2010BUJICT

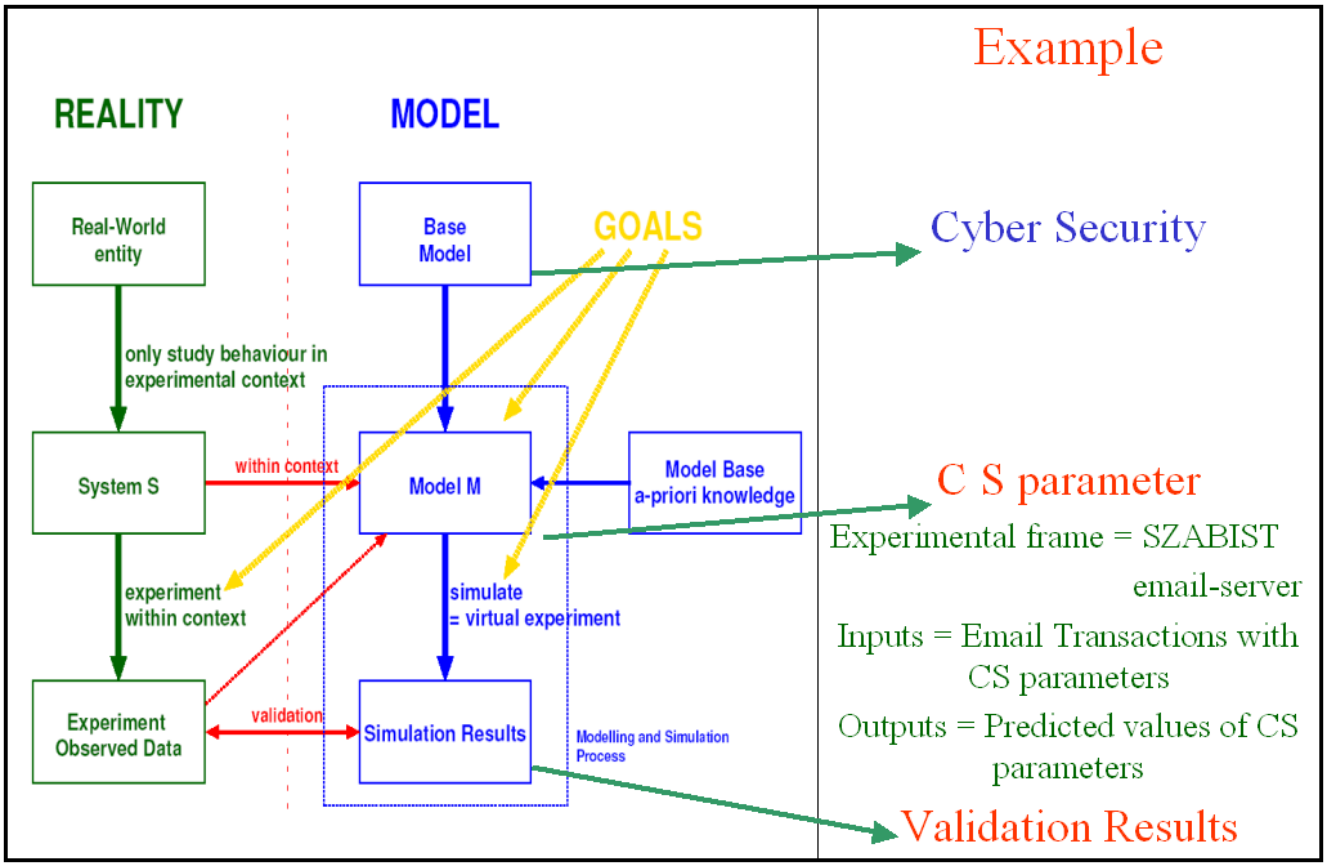

Fig.7. Simulation Model Process

TABLE III
ATTACKS, RISKS, VULNERABILITIES AND RELATED CONSEQUENCES DATA

Type of attack	Risk	Vulnerability	Consequence
Denial of Service	Flood Router	No Firewall	Prevent legitimate users of a service from using it
Virus	Corrupt Operating System	No Anti Virus Software	Operating System Rendered Inoperable
Probe	Obtain Web Server Account Information	No Web Server Firewall	Web Server programs Hijacked
Account Compromise	Capture Account	No proper account policy	Unauthorized use of user account
Packet Sniffer	Capture Passwords	No Password Capture Protection	Passwords Compromised
Root Compromise	Discover information about the system	No proper privileges	Account compromised has privileges
Trojan Horse	Hide in Host and Corrupt Applications	No Software to detect Trojan Horse	Hidden in legitimate programs or files
Worm	Replicates itself	No Anti Worm Software	Spread with no human intervention
Spyware	Unauthorized Access	No Anti Spyware Software	Permits unauthorized access to a computer
Corruption of Database	Database Corrupted	No Database	Data is rendered unrecognizable