**A Case Study on Attack Vector**

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Keywords---Cyber Vulnerability, patching, hacker, Probability,

cyber Random Space, Patch Application time, compromised

employee.

I. INTRODUCTION

There is adequate randomness in the reporting of

cyber vulnerability and as expected there would be remedies

being reported at equally random intervals. India ranked

highest in terms of Spam Zombies activity in 2012-13 as

published in the Symantec report [1]. As per Symantec, it

blocked a total of over 5.5 billion malware attacks in 2011[2].

There was an increase in web based attacks to over 4,500

new attacks each day. And similarly on an average 82

targeted attacks take place each day and 403 million new

variants of malware were created in 2011. Keeping in view

the enormity of the challenge there is a need to quantify the

vulnerability in a probabilistic manner. There is bound to be

randomness in the way vulnerability patch is applied by any

user. This paper will attempt to understand various paths that

could be used to mount an attack and their probability.

Vulnerability may refer to some known or unknown

weakness in the cyber network system that can be exploited

to modify or misuse the system which is not its intended use.

Any typical network would consist of computers,

communication systems, a central server, functional database

and access system that may wired or wireless. Any person

who has good knowledge of these systems can interfere with

them once access is permitted. Every network will comprise

of large number of networked computers with stated charter.

Computer performing critical functions need protection in

order to avoid any interruption in overall process.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Keywords---Cyber Vulnerability, patching, hacker, Probability,

cyber Random Space, Patch Application time, compromised

employee.

I. INTRODUCTION

There is adequate randomness in the reporting of

cyber vulnerability and as expected there would be remedies

being reported at equally random intervals. India ranked

highest in terms of Spam Zombies activity in 2012-13 as

published in the Symantec report [1]. As per Symantec, it

blocked a total of over 5.5 billion malware attacks in 2011[2].

There was an increase in web based attacks to over 4,500

new attacks each day. And similarly on an average 82

targeted attacks take place each day and 403 million new

variants of malware were created in 2011. Keeping in view

the enormity of the challenge there is a need to quantify the

vulnerability in a probabilistic manner. There is bound to be

randomness in the way vulnerability patch is applied by any

user. This paper will attempt to understand various paths that

could be used to mount an attack and their probability.

Vulnerability may refer to some known or unknown

weakness in the cyber network system that can be exploited

to modify or misuse the system which is not its intended use.

Any typical network would consist of computers,

communication systems, a central server, functional database

and access system that may wired or wireless. Any person

who has good knowledge of these systems can interfere with

them once access is permitted. Every network will comprise

of large number of networked computers with stated charter.

Computer performing critical functions need protection in

order to avoid any interruption in overall process.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Keywords---Cyber Vulnerability, patching, hacker, Probability,

cyber Random Space, Patch Application time, compromised

employee.

I. INTRODUCTION

There is adequate randomness in the reporting of

cyber vulnerability and as expected there would be remedies

being reported at equally random intervals. India ranked

highest in terms of Spam Zombies activity in 2012-13 as

published in the Symantec report [1]. As per Symantec, it

blocked a total of over 5.5 billion malware attacks in 2011[2].

There was an increase in web based attacks to over 4,500

new attacks each day. And similarly on an average 82

targeted attacks take place each day and 403 million new

variants of malware were created in 2011. Keeping in view

the enormity of the challenge there is a need to quantify the

vulnerability in a probabilistic manner. There is bound to be

randomness in the way vulnerability patch is applied by any

user. This paper will attempt to understand various paths that

could be used to mount an attack and their probability.

Vulnerability may refer to some known or unknown

weakness in the cyber network system that can be exploited

to modify or misuse the system which is not its intended use.

Any typical network would consist of computers,

communication systems, a central server, functional database

and access system that may wired or wireless. Any person

who has good knowledge of these systems can interfere with

them once access is permitted. Every network will comprise

of large number of networked computers with stated charter.

Computer performing critical functions need protection in

order to avoid any interruption in overall process.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

Abstract---Current day networks operate on multiple hardware

devices assisted by numerous numbers of operating systems.

Systems may have vulnerabilities. These are explored and then

exploited. Among the overall malicious activity countries, India

ranked third after US and China. This paper has made an

attempt to explore possibility of quantifying various

probabilities. Cyber system can be modeled in different ways.

There are various attack vectors that make cyber network

vulnerable. A compromised employee is an insider to any

network and contributes significantly to the network

vulnerability. Keeping in mind various random variables that

affect the safety of Cyber Random Space, there may be a need to

quantify the probability associated with different cyber

exploitation related activities.

**Abstract**

Current day networks operate on multiple hardware devices assisted by numerous numbers of operating systems. Systems may have vulnerabilities. These are explored and then exploited. Among the overall malicious activity countries, India ranked third after US and China. This paper has made an attempt to explore possibility of quantifying various probabilities. Cyber system can be modeled in different ways. There are various attack vectors that make cyber network vulnerable. A compromised employee is an insider to any network and contributes significantly to the network vulnerability. Keeping in mind various random variables that affect the safety of Cyber Random Space, there may be a need to quantify the probability associated with different cyber exploitation related activities.

**INTRODUCTION**

There is adequate randomness in the reporting of cyber vulnerability and as expected there would be remedies being reported at equally random intervals. India ranked highest in terms of Spam Zombies activity in 2012-13 as published in the Symantec report [1]. As per Symantec, it blocked a total of over 5.5 billion malware attacks in 2011[2]. There was an increase in web based attacks to over 4,500 new attacks each day. And similarly on an average 82 targeted attacks take place each day and 403 million new variants of malware were created in 2011. Keeping in view the enormity of the challenge there is a need to quantify the vulnerability in a probabilistic manner. There is bound to be randomness in the way vulnerability patch is applied by any user. This paper will attempt to understand various paths that could be used to mount an attack and their probability. Vulnerability may refer to some known or unknown weakness in the cyber network system that can be exploited to modify or misuse the system which is not its intended use. Any typical network would consist of computers, communication systems, a central server, functional database and access system that may wired or wireless. Any person who has good knowledge of these systems can interfere with them once access is permitted. Every network will comprise of large number of networked computers with stated charter. Computer performing critical functions need protection in order to avoid any interruption in overall process.

**CYBER RANDOM SPACE**

The term queuing denotes a large scale phenomena which includes arrival process, waiting for the service, servicing and then leaving the queue after receiving the service. Cyber space can be considered as a random space where vulnerabilities are reported at regular interval. In this space, vulnerabilities are reported at regular intervals. As soon as vulnerability is reported, process of developing a security patch is taken up by various agencies. There is delay of finite time interval before a patch is developed. Even if we consider patch deployment time to be negligible, there is a definite delay before a user is made aware of the vulnerability patch and encouraged to apply it to the system. As there are various types of vulnerabilities and large clientele base, the delay in application of patches is an opportunity for a hacker. For a vulnerability arrival queuing process, if N is No of vulnerabilities in cyber system at any one time, λ is rate of arrival (reporting) of vulnerabilities and T is time spent by the vulnerability in the system before being serviced then by application of Little’s theorem we can arrive at relation Ν=λΤ . This gives an estimate as to how much vulnerability remains in the system at any one time. N will keep increasing linearly as delays in patching (T) increase. Simulation model as proposed in [3] was used to study the relation among patching time, size of network, state of initial infection etc. In the simulation result below, infection was allowed to spread for sufficiently large time t=1200 sec with very low (just two) initial infected computers. An assessment about number of infected computers with lapse of time revealed that there is approximately a linear relationship indicating the infection and patching. It was assumed that there were 10,000 fully connected computers in network. As the infection time is reduced the number of infected PCs also reduces rapidly. Hence low patch application delay time is very helpful in reducing the vulnerability.

**CYBER ATTACK VECTORS**

Internet has become vulnerable due to large number of attack vectors being exploited on regular basis. Attack vectors use various resources to infect the computer and other networking devices ensuring the passage to intended target/ information.

Some of the attack vectors that have been analysed are as under:-

• Compromised Employee.

• Infection through email.

• Third party systems and Packages.

• Infection through the removable media.

• Attack on Mobile Device.

• Targeted attacks on user network.

A. **Compromised Employee**

An insider in any organization can pose threat if compromised. There are cases when an employee was bribed to obtain privileged network information. This information was later used by an attacker to exploit the systems and gain unauthorized access in to the network. There has been an attempt to quantify the risk assessment due to bribing incident by Hunt J in [4]. It was indicated that various factors such as payments in cash or service, age, country, culture, salary etc contribute towards bribery risk assessment. Considering all relevant factors Hunt estimated the probability of Bribery as 12%. Compromising an employee may guarantee the delivery of vulnerable services (considered 100% success). However job satisfaction within the company or organization may be an important factor to determine the final outcome. Hezerberg [5] analysed main factors determining effectiveness of employee as working conditions, supervision, Company Policy, administration and salary. It was indicated in [6] that job satisfaction could be assumed to be 79% as there was an overall variance in data by 21%. Hence probability that a compromised employee will successfully deliver the intended vulnerability within the system can be pegged at 79%. Hence Probability that a compromised employee will cause cyber attacks in Pc = 79%.

B. **Probabilistic Epidemic Outbreak Model**

Cyber exploitation exhibits properties very similar to an epidemic outbreak. I draw a parallel between the two as both spread in a similar manner. Both experience an outbreak, need to sustain above a threshold level, are caused by external agents and need a time critical removal response depending on the nature of infection. Lets us consider a class of healthy clients that are susceptible to infection C (t) at any time‘t’, Infected clients (Hacked and currently compromised), H (t) and sanitized clients S(t), which were infected but now cleaned and all precautions taken. It is assumed that sanitized clients will not participate in further infection and no more a subset of C (t). We assume infection rate at any time‘t’ to be α (t) and β (t) to be the rate of removal of infection. It is assumed that clients can transparently communicate with each other and sanitized class does not participate in the spreading the cyber virus. Total number of clients that will be available at any time t, T(t)= C(t) +H(t) +S(t). If n is the number of contacts an infected machine makes and µ is the capability of a client to infect other healthy workstations then infection rate = nµ/T (t). H(t).

C. **Single Epidemic Outbreak**

Considering the case of single out break for a limited time, assuming that number of work stations remain same in the network during infection then occurrences can be identified as change in number of susceptible C’(t) = -α(t). C(t) with boundary conditions C(0) = C0. Similarly, infection rate H’(t) = - β(t).H(t) + α(t).C(t), H(0)=H0 and rate of immunization S’(t)= - β(t).H(t), S(0)=S0. With the boundary conditions, the rate of removal of infection will be given by H'(t) = [α C(t)-β]H(t).

D. **Infection through Email**

There is a definite probability of infecting a PC using email worms. There are various methods which have been used to estimate propagation of email worms. Use of graph theory [9] and use of epidemiological equation [10] and branching theory. Propagation of email worms may have following distinct attributes:- • Crossing over the email server spam filter. • Detection by antivirus program. • Number of attempts by user to open infected mail. Crossing over the spam filter is an important event. Hackers use media engineering technique to ensure smooth Passover of infected mails as legitimate ones. Email messages are made as realistic as possible with minimum number of attempts to execute the malware code.

E. Third Party Systems and Packages

Third party systems would broadly include all the

applications and resources available over the web servers

which could be accessed over network. There is a way

envisaged about the propagation of worm/virus. First of all

we assume that cyber hackers are capable of continuously

uploading infected files to create more and infection sources.

Faster the propagation, better would be the infection

response. Stuxnet worm infected 14000 hosts in 72 hours

[17].

E. **Third Party Systems and Packages**

Third party systems would broadly include all the applications and resources available over the web servers which could be accessed over network. There is a way envisaged about the propagation of worm/virus. First of all we assume that cyber hackers are capable of continuously uploading infected files to create more and infection sources. Faster the propagation, better would be the infection response. Stuxnet worm infected 14000 hosts in 72 hours [17].

**CONCLUSION**

As evident from the discussions in above mentioned paragraphs probabilistic modeling of attack on a network is a complex issue. More so because of an inter-dependence among attack vectors is a prerequisite to launch successful attack. A highly skilled attacker is more likely to be ready for unexpected exploits than a novice or semi skilled attacker. However same may not always be true. In addition there are large number of attack vectors which need to be considered to arrive at a comprehensive mathematical model.