e-Epidemic models on interaction between malicious codes and anti-virus software

Bimal Kumar Mishra, Ph. D., D.Sc.
Department of Applied Mathematics
Birla Institute of Technology,
Mesra, Ranchi – 835 215
Email:
drbimalmishra@gmail.com

INTRODUCTION

- A year or two year before computer viruses spread through email and EXE file
- Now preferred way of spreading malware is by drive-by-drive download or email spam connecting through link
- Transmission of malicious objects in computer network is epidemic in nature

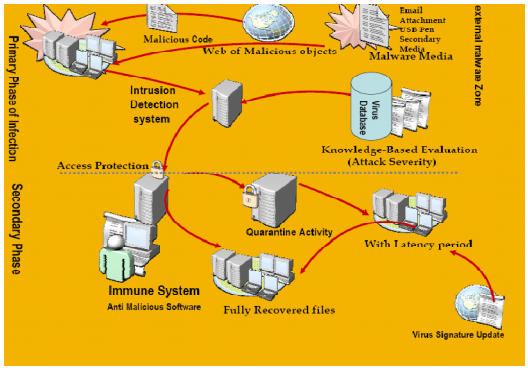
INTRODUCTION

- Attacking nature is different for different types of malicious code
- Different nature or classification of computer malware exist
- The study of computer may help to control infectious disease emergence
- Different kind of viruses exist like 'Logic Bomb' , 'Parasitic'

INRODUCTION

- Malicious code is treated through a model which comprise of IDS (Intrusion Detection System),ADS and Knowledge based system vulnerability information system
- The model is described in the next slide

Virus attack cyber defense analysis



BASIC TERMINOLO G IES

- **Computer virus** is a program that can "infect" other programs by modifying them to include a possibly evolved version of it
- **Antivirus (or "anti-virus") software** is a class of program that searches your hard drive and floppy disks for any known or potential viruses.
- **Quarantine:** To move an undesired file such as a virus-infected file or spyware to a folder that is not easily accessible by regular file management utilities.

What are malicious objects?

- The term "gateway" refers in the art to a bridge between two networks. For each network, the gateway is a point that acts as an entrance to another network
- As a filtering facility, a gateway server has to be dealt with two contradicting objects: on the one hand, it has to hold a file that reaches the gateway in its path from a source to a destination until the inspection indicates it is harmless and thereby prevents its execution on the destination site, on the other hand holding a file at the gateway server until the inspection process terminates which results in a bottleneck to data traffic passing through the gateway. Inspection activity has a substantial influence on the traffic speed through a gateway

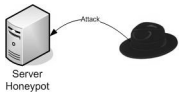
What are malicious objects??

- Obviously hiding presence of a malicious program is more advanced than the non-hidden attack. The big threat it poses is the invisibility. The hidden process won't be seen in Task Manager. Beyond that the ordinary anti-spyware and anti-virus tool are not able to detect them either

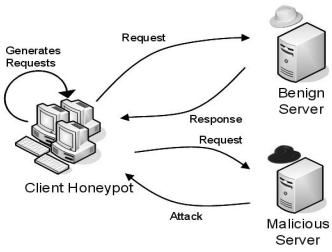
What is malicious objects??

- At the heart of this vulnerability is the violation of trust that results from the "injected" script or HTML running within the security context established for the example.com site. It is, presumably, a site the browser victim is interested in enough to visit and interact with in a trusted fashion. In addition, the security policy of the legitimate server site example.com may also be compromised.

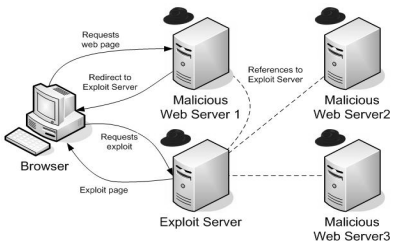
Malicious objects-Facts



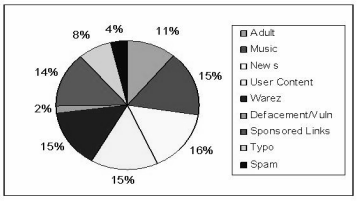
Malicious objects-Facts



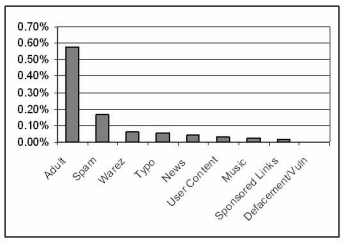
Malicious objects-Facts



Malicious objects-Facts



Malicious objects-Facts



DEVELOPMENT OF THE MODEL

- Set of Instructions written by the User to harm the system is said to be the 'Virus' which attack the computer
- Some of the virus self-replicating in nature
- Some of them enter in the latent class and reactivate after certain duration
- Antivirus software immune the system if it is attacked by the virus

DEVELOPMENT OF THE MODEL

- During immunization some of the infected files get fully recovered, whereas, some of them are quarantined (or suppressed), may be due to the lower version of the antivirus software installed.
- Then for this situation a higher version or new antivirus software is run to get a full recovery
- We try to develop Mathematical models for these situations

DEVELOPMENT OF THE MODEL

- Virus is replicated by the infected files.
- Viruses die at a specific rate b. Death of a virus equivalently mean to say the complete recovery of infected files from virus when antivirus software is run in the computer node for a specific session.
- The uninfected files are constantly being produced or developed by the users at a rate c.
- Uninfected files die at a constant rate d (natural death). Death of a file equivalently mean to say that the file become irrelevant (garbage) after a certain interval of time.

DEVELOPMENT OF THE MODEL

- Infected files die at a specific rate, where d is natural death rate and e the death rate of the file (files get damaged and unable to be recovered after the run of antivirus software)due to infection from the virus.
- Death of antivirus software equivalently mean to say the present version of the software is incapable of identifying the attack of new viruses.

Model 1: Primary phase of an Infection

- Viruses get entry to the computer node via various means (emails, infected disks etc.) and hijack various files (command files, executable files, kernel.dll, etc.) in the node for its own replication.
- It then leaves a specific file and the process is repeated.
- Viruses may be of different nature and as per their propagation mode; they target different file types of the attacked computer for this purpose.

Model 1: Primary phase of an Infection

$$\frac{dV}{d\tau} = aY - bV$$

$$\frac{dX}{d\tau} = c - dX - \beta XV$$

$$\frac{dY}{d\tau} = \beta XV - fY$$

Model 1: Primary phase of an Infection

- Let X be the number of uninfected files (prey) and V be the number of computer virus (predators), then
- {Rate of change of X}= {net rate of growth of X without predation}-{rate of loss due of X to predation, and
- {Rate of change of V}= {net rate of growth of V due to predation}-{net rate of loss of V without prey}

Model 1: Primary phase of an Infection

- Let, R_0 be the basic reproductive ratio for the computer virus; defined to be the expected number of viruses that one virus gives rise to an uninfected file population. A virus gives rise to infected files at a rate βX for a time 1/b, and each infected files gives rise to virus (self replication) at a rate *a* for a time 1/f. since X=c/d for a uninfected population,

$$R_0 = \frac{\beta ca}{dbf}$$

The criterion for the spread of the computer virus is

$R_0>1$

Model II: Secondary Phase of Infection (Effect of Immune system)

- We assume the response of the immune in the computer system due to antivirus software Z which are run at a constant rate g and h being the death rate of antivirus software
- The antivirus software cleans the infected files at a rate
- There is an analogy here of Z antivirus software as predators and Y infected files as prey
- We take linear functional response of Z to Y

Model II: Secondary Phase of Infection (Effect of Immune system)

$$\frac{dV}{d\tau} = aY - bV$$

$$\frac{dX}{d\tau} = c - dX - \beta XV$$

$$\frac{dY}{d\tau} = \beta XV - fY - \gamma YZ$$

$$\frac{dZ}{d\tau} = g - hZ$$

3.3 Model III: Effect of new antivirus software on such viruses which are suppressed (quarantine)

We assume a case where the viruses are not completely cleaned (quarantine) from the infected files on run of installed antivirus software on the computer node. For the complete recovery of infected files from viruses, updated version of antivirus has to be run. Further we assume that such updated antivirus software is available and is 100% efficient. This antivirus software switches β to zero and thus the equations for the subsequent dynamics of the infected files and free virus from equation (1) is expressed as

$$\frac{dV}{d\tau} = aY - bV$$
$$\frac{dX}{d\tau} = c - dX$$
$$\frac{dY}{d\tau} = -fY$$

We further assume that the half-life of the virus is much less than that of the virus producing files. Then,

$$Y = Y_0 e^{-ft}$$
$$V = \frac{V_0 (be^{-ft} - fe^{-bt})}{(b - f)}$$

From equation (14) we are able to say that the number of infected files falls exponentially. The behavior of V follows from the assumption on half-lives, so that

, $f << b$

that is, the amount of free virus falls exponentially after a shoulder phase.

Model IV: Reactivation of computer virus after they are in latent class

When computer virus attacks the computer node, some of them enter a latent class on their infection. While in this class they do not produce new viruses, but may later be reactivated to do so. Only the files in the productive infected class Y1 produce viruses, and files at latent infected class Y2 leave for Y1 at a per capita rate d. Thus our system becomes:

$$\frac{dV}{d\tau} = aY_1 - bV$$
$$\frac{dX}{d\tau} = c - dX - \beta XV$$
$$\frac{dY_1}{d\tau} = q_1 \beta XV - f_1 Y_1 + \delta Y_2$$
$$\frac{dY_2}{d\tau} = q_2 \beta XV - f_2 Y_2 - \delta Y_2$$

Infected files at class Y_2 produce viruses in class Y_1 at a rate δ for a time $\frac{1}{\delta + f_2}$

Thus adding the contribution of both the classes, the reproductive ratio R_0 is expressed as

$$R_0 = \frac{\beta c}{db}\left(q_1 + q_2 \frac{\delta}{\delta + f_2}\right)\frac{a}{f_1}$$

3.5 Model V: Recent Attack by malicious object Backdoor.Haxdoor.S and Trojan.Schoeberl.E and its Mathematical approach

On January 9, 2007 *Backdoor.Haxdoor.S* and *Trojan.Schoeberl.E* malicious object of type *Trojan Horse* having infection length of 56,058 bytes affected Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP. Backdoor.Haxdoor.S is a Trojan horse program that opens a back door on the compromised computer and allows a remote attacker to have unauthorized access. It also logs keystrokes, steals passwords, and drops rootkits that run in safe mode.
It has been reported that the Trojan has been spammed through email as an email attachment. The tool ***FixSchoeb-Haxdoor.exe*** is designed to remove the infections of *Backdoor.Haxdoor.S* and

FixSchoeb-Haxdoor.exe tool meant to remove the deadly *Backdoor.Haxdoor.S* and *Trojan.Schoeberl.E* prevent infected files from producing infectious virus. We assume that W are the un- infectious virus which start to be produced from the infected files Y after the tool *FixSchoeb-Haxdoor.exe* is run. Infectious virus are still present, and die as before, but are no longer produced. Under this assumption the system can be modeled as

Discussion and Conclusion

The threshold parameter obtained in (2) for primary phase of i
discusses the criterion for the spread of the computer virus, that i

. The susceptible population X (uninfected files) is reduced by th
until each virus is expected to give rise to exactly one new virus,

. The basic reproductive ratio in the presence of the immune sy
defined by (11) and in order for the immune response to c
infection we need the immune response parameter κ
to satisfy $\kappa > \alpha(R_0 - 1)$
For the viruses which are quarentined by the installed antivirus s
we assume that updated antivirus software is available and i
efficient. When this updated antivirus software is run, from equat
we are able to say that the number of infected files falls expon
The behavior of V follows from the assumption on half-lives, so th

We assume that the uninfected file population X remains roughly constant for a given time-scale, that is,

$X = X^* = \frac{bf}{a\beta}$ and that $f << b$

System (17) becomes a linear system which is integrated to have

$$V = V_0 e^{-b\tau}$$

$$Y = Y_0 \frac{fe^{-b\tau} - be^{-f\tau}}{f - b} \quad ,when \quad f << b$$

$$W = W_0 \frac{b}{b-f}\left(\frac{b}{b-f}(e^{-f\tau} - e^{-b\tau}) - f\tau e^{-b\tau}\right)$$

From (18) it is clear that the total amount $V + W$

of free virus falls exponentially after a shoulder phase.

Nomenclature

V : number of viruses in the computer
X : number of uninfected target files
Y : number of infected files
A : Replicating factor
B : Death rate of a virus
C : Birth of uninfected files by users
D : Natural Death of an uninfected file
E : Death rate of infected files
f = e + d
β : Infectious contact rate, i.e., the rate of infection per susceptible and per infective
R0 : Threshold parameter
Z : Response of antivirus software, which immunes the system
G : Rate at which antivirus software is run, which is

DISCUSSION AND CONCLUSION

- The threshold parameter obtained for primary phase of infection discusses the criterion for the spread of the computer virus, that is, $R_0 > 1$
- The susceptible population X (uninfected files) is reduced by the attack until each virus is expected to give rise to exactly one new virus,
- The basic reproductive ratio in the presence of the immune system is defined Model II and in order for the immune response to clear the infection we need the immune response parameter to be more than secondary phase of infection

REFERENCES

- Bimal Kumar Mishra, D.K Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer network, Applied Mathematics and Computation, 188 (2007) 1476-1482
- Bimal Kumar Mishra, Dinesh Saini, Mathematical models on computer viruses, Applied Mathematics and Computation, 187 (2007) 929-936
- Lotka, A. J., Elements of Physical Biology, Williams and Wilkins, Baltimore, 1925; Reissued as Elements of Mathematical Biology, Dover, New York, 1956.

REFERENCES

- Volterra, V., Variazioni e fluttazioni del numero d'individui in specie animali conviventi, Mem. Acad. Sci. Lincei, 1926, 2:31-13
- Jones, A.K. and Sielken, R.S., Computer System Intrusion detection: a survey, Technical report, Computer Science Department, University of Virginia, 2000
- Yu, J., Reddy, R., Selliah, S., Reddy, S., Bharadwaj, V. and Kankanahalli S., TRINETR: An Architecture for Collaborative Intrusion Detection and Knowledge-Based Alert Evaluation, In Advanced Engineering Informatics Journal, Special Issue on Collaborative Environments for Design and Manufacturing. Editor: Weiming Shen. Volume 19, Issue 2, April 2005. Elsevier Science, 93-101

REFERENCES

- Jinqiao Yu, Y.V.Ramana Reddy , Sentil Selliah, Srinivas Kankanahalli, Sumitra Reddy and Vijayanand Bhardwaj, A Collaborative Architecture for Intrusion Detection Systems with Intelligent Agents and Knowledge based alert Evaluation, In the Proceedings of IEEE 8th International Conference on Computer Supported Cooperative work in Design, 2004, 2: 271-276
- Nicholas F. Britton, Essential Mathematical Biology, Springer-Verlag, London, 2003
- Bimal Kumar Mishra , Navnit Jha, Fixed period of temporary immunity after run of anti-malicious objects software on computer nodes, Applied Mathematics and Computation, 190 (2007) 1207-1212

REFERENCES

- http://www.symantec.com/smb/security_response/writeup.jsp?docid=2007-011109-2557-99
- Masud, Mohammad M., Khan, Latifur and Thuraisingham, Bhavani, A Knowledge-based Approach to detect new Malicious Executables. In the proceedings of the Second Secure Knowledge Management Workshop (SKM) 2006, Brooklyn, NY, USA
- http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html, March 31, 2008

THANK YOU