Network and Communication Technologies; Vol. 1, No. 2; 2012
ISSN 1927-064X E-ISSN 1927-0658
Published by Canadian Center of Science and Education

Using Simulation to Investigate Virus Propagation in Computer Networks

Arben Asllani[1] & Amjad Ali[2]

[1] College of Business, University of Tennessee at Chattanooga, Chattanooga, Tennessee, USA

[2] Center for Security Studies, University of Maryland University College, Adelphi, Maryland, USA

Correspondence: Arben Asllani, College of Business, University of Tennessee at Chattanooga, Chattanooga, Tennessee, USA. Tel: 1-423-425-4412. E-mail: beni-asllani@utc.edu

Received: October 17, 2012 Accepted: November 6, 2012 Online Published: November 23, 2012

doi:10.5539/nct.v1n2p76 URL: http://dx.doi.org/10.5539/nct.v1n2p76

Abstract

Making the best decisions to respond to a virus threat can be critical in thwarting a quick spread and minimizing negative impacts of an attack. This paper uses simulation to compare two main prevention strategies: patching and quarantine. These strategies are borrowed from epidemiological models and are currently employed to prevent and control the spread of computer viruses throughout networks. Simulation is a powerful decision making tool which can be used to mimic the complex behavior of a spreading virus while testing a range of alternative parameters for different attack scenarios. The proposed simulation model suggests that patching is a better protection strategy than quarantine. A carefully selected patching strategy can be used to enforce the herd immunity effect and place the spread of a virus in an endemic state in the shortest possible amount of time.

Keywords: virus, propagation, simulation, patching, quarantine

1. Introduction

The rapid development of computer connectivity and the dependence of organizations on the new e-commerce markets have increased vulnerabilities of networks. There is a persistent threat of malware programs and its growth has become exponential (Cobb & Myers, 2009). The large number of existing computer viruses and their highly destructive nature to harm computer systems appear as an important security risk for both organizations and individuals. Computer viruses are basically computer programs created to damage the computer systems, erasing data, stealing information and altering the normal operations of computer systems (Piqueira et al., 2008). Establishing appropriate protection policies and implementation of realistic plans of actions are as important as antivirus technology used to thwart an attack. The main goal of these policies is to protect the network, guard organizational data, and continue to support organizational transactions.

Several studies have suggested the use of epidemiology models to understand the spread of viruses in computer networks and to design appropriate response strategies (Kephart & White, 1991; Pastor-Satorras & Vespignani, 2002). Recently, Mulligany and Schneider (2011) made the case that cyber security can be viewed as a "public good" and suggest the adoption of mechanism and strategies derived from public health.

No matter how well prepared a protection plan may be, it cannot be proven effective until is put to test or verified. While an actual infection will highlight failures of a given plan, simulation methodology shows high potential for studying and investigating response strategies. Unlike actual infections, simulation models are less expensive, take less time to be conducted, and are well suited for testing alternative solutions. The decision makers can modify and analyze the model in order to test and evaluate numerous scenarios and operating parameters.

This paper uses simulation as a decision making tool to replicate the spread of a virus in a computer network. The simulation model is based on mathematical foundations of epidemiological theory. Specifically, the model investigates the impact of different degrees of patching and quarantine on the spread of the virus and suggests optimal parameters which utilize the impact of herd immunity. These two strategies are borrowed from epidemiological models (vaccination and isolation) and are currently employed to prevent and control the spread of computer viruses throughout networks.

The paper is organized as follows: The next section offers a brief discussion of previous research in the areas of

epidemiology, its mathematical model, and its potential use to model the spread of computer viruses. The next section explains the simulation approach, input/output variables, and its main algorithm. Once the model is validated, several experiments are conducted to investigate the impact of patching and quarantine. Finally, conclusions and future research are discussed.

2. Previous Research

The proposed simulation model is based on the assumption that a computer virus is spread throughout a network in the same way that a disease spreads in a population. As such, the first part of this section discusses the theory of epidemiology. The first complete discussion of mathematical epidemiology is offered by McKendrick (1925) in his paper presented at the Edinburgh Mathematical Society. A few years later, McKendrick and Kermack offer the basic compartmental models and mathematically describe the transfer rate of individuals from one compartment to the next using a set of partial differential equations (Kermack & McKendrick, 1927; Kermack & McKendrick, 1932). A more complete work of mathematical epidemiology is summarized in the work of Bailey (1975) and Frauenthal (1980).

Focusing on pandemic influenza, Larson and Nigmatulina (2009) use simple mathematical models to discuss courses of actions for response to major worldwide health events. Specifically, the authors employ simple mathematical models and use the "reproductive number" concept to suggest strategies to control the spread of the disease. They conclude, for example, that any numerical value for the reproductive number has "little meaning outside the social context to which it pertains" and their analysis shows the disease tends to be driven by high frequency individuals. The model discussed by Larson and Nigmatulina (2009) assumes a homogenous mixing of population. Homogeneous mixing is a reasonable assumption to simplify the mathematics of the model. More advanced models assume non-homogeneous mixing of population. For example, Hill and Longini (2003) describe a mathematical model, which optimally allocate vaccines to several subpopulations with potentially heterogeneous mixing of individuals.

Mathematical models are also used to depict the impact of vaccination rate on the spread of disease. Two of the most important theoretical concepts in infectious disease epidemiology are the basic reproduction number and herd immunity. The models following the theory regarding reproduction number come very close to determining the required vaccination coverage for eradication in a randomly mixed population (Anderson & May, 1991; Diekmann & Heesterbeek, 2000). These models were later extended to include such factors as non-homogenous distribution of population and contacts, contact tracing, and ring vaccination (Fine, 1993), which is the vaccination of all susceptible individuals around an outbreak.

Another aspect of vaccination models is the concept of herd immunity. Due to herd immunity, vaccination can also help protect people who are not vaccinated. The unvaccinated people in the herd community can escape the infection because they are protected by the immunized people who surround those (Anonymous, 2011). Immunity against a disease can be acquired either through natural infection or through artificial inoculation with a vaccine (Garnett, 2005).

Detailed mathematical models of diseases are common in medicine but rare in digital security (Geer & Conway, 2009). Kephart and White published a paper on the topic in 1991 and model the spread of viruses or other malware between hosts using the same methodology provided in the epidemiological models (Kephart & White, 1991). Zou, Gong, and Towsley (2003) present a mathematical analysis of three worm propagation models under a dynamic quarantine environment. The worm propagation based on quarantine is further investigated in three more recent papers. Chen and Jamil (2006) study the effectiveness of partial quarantine for simple epidemics (without removals) and quarantine for general epidemics (with removals) and derive a critical threshold for networks to have herd immunity. Also, Tao, Weng, and Zhu (2008) propose a worm propagation model with quarantine strategy and provide mathematical foundations to study of global stability of equilibriums of the model. Chen and Wei (2009) offer improvements of classical susceptible-infected-susceptible and susceptible-infected-recovered models with quarantine strategy, thresholds and equilibriums to the existence of worm epidemics. More recently, Wang et al. (2010) propose an epidemic model combining both vaccinations and quarantine methods to decrease the number of infected hosts and reduce the speed of worm propagation.

Network analysis is another approach to investigate the spread of a disease. In these networks nodes represent people, and edges represent specified relationships or interactions. Studies which use networks to simulate the spread of the disease from one source node to the rest of population have shown that the "betweenness" and the "farness" of nodes alter disease dynamics (Christley et al., 2005). The simulation model proposed in this paper is based on the mathematical foundations of the epidemiology. The model considers herd immunity and several other key factors, such as reproduction number, transmission period, patching (vaccination) rate and quarantine

(isolation) rate. These factors are incorporated into a network based simulation model. The goal is to represent the complexity of the model into a practical simulation based decision making tool for evaluating alternative response strategies.

3. Mathematical Foundations of the Simulation Model

A host is a computer or device which is connected to other computers or devices in a given network. The host is able to forward a virus to other connected hosts in the network. In this paper we assume homogeneous mixing of the hosts, that is, hosts in the network under scrutiny make contact at random and do not mix solely in a smaller subgroup. Denoting the initial number of infected hosts by h, the number of connections or reproduction number by R_o, and the generation number by n, the number of infected host increases according to the following series:

$$h, hR_o^2, hR_o^3, \ldots, hR_o^n \tag{1}$$

Starting with a single initial infected host, the number of infected hosts in the n^{th} generation is equal to the number of connections to the power of n. This exponential growth assumes that the infection ratio is the same as the number of connections. However, as the virus continues to spread in the network from one generation to the next, infected hosts are no longer susceptible to the virus. The infection ratio or the number of hosts infected in the next generation from a single infected host changes as the model progresses through generations and is calculated as:

$$I = R_0 \frac{S}{P} \tag{2}$$

Where:

- I = number of hosts infected from a single infected host in a given generation
- R_o = number of initial contacts in the network group
- S = number of susceptible hosts in the network group in the generation
- P = number of hosts in the network group, also referred as the size of network

When $I=1$ the spread of the virus is considered to be in an endemic mode. This means that on average, each infected host is infecting exactly one other host. From a network administrator perspective, the virus can be sustained by lowering the number of susceptible hosts by increasing the number of patched hosts. If $I>1$ the virus is considered to be in an epidemic state, and the number of hosts infected grows exponentially. If $I<1$ the disease will die out. The virus is contained when the number of hosts infected from a single infected host must be either less than or equal to 1. As such:

$$I = R_0 \frac{S}{P} \leq 1 \tag{3}$$

Formula (3) indicates that in order to eliminate the virus or keep it in an endemic state, the number of susceptible hosts must be kept lower than or equal to the ratio between network size and the reproduction number, as follows:

$$S \leq \frac{P}{R_0} \tag{4}$$

Formula (4) indicates the rationale of a patching program: in order for any course of action to work, enough hosts must be patched so that the number of susceptible hosts (S) is kept below the threshold. If V represents the number of hosts to be patched before the first infection occurs, then $S=P-V$. Replacing S in (4), the lower boundary for V can be calculated as variable V_m:

$$V_m = \frac{P(R_0-1)}{R_0} \tag{5}$$

For example, in a network with 900 computers where each computer is connected and can infect an average of three other computers, the network administrator must patch at least 600 computers to keep the virus from spreading.

Besides patching, quarantine is an alternative method to control the spread of the virus. By isolating the infected hosts, the number of connections which can spread the virus is in fact reduced. Continuing with the above example and assuming that quarantine is the only course of action, and that the isolation of infected computers can lead to an average of two actual infectious connections, the system administrator must quarantine up to 450 computers after they are infected.

The above mathematical explanation is used to identify the minimum number of hosts to be patched or isolated in a deterministic environment. Formula (5) can be used successfully when number of connections is already

known in advance. While in a typical network topology each hosts is physically connected to every other host, the actual connections to be considered in the model is in fact a stochastic variable. A connection between two computers is "virtual". A connection between two hosts exists if there is a communication between the two while any of them is infected. As such, the spread of the virus in a network can be better represented as stochastic model via simulation. Simulation methodology can not only be used to estimate the minimum number of hosts to be patched or isolated in a given network, but also to investigate strategies which can minimize the number of infected hosts during a virus attack.

4. Conceptual Simulation Model

This research offers a simulation model which can be used by practitioners as an effective decision making tool to identify appropriate virus mitigation strategies based on network characteristics. Simulation uses a logical abstraction of the reality through a computer model that "mimics" the behavior of the virus as it spreads through the network. Once the computer based simulation model is validated, the decision maker can test a range of alternative solutions for different scenarios. In addition, the robustness of the alternative solutions can be tested by "tweaking" the model to reflect changes in the parameters of the system.

The basis for the conceptual design of the proposed simulation model is the Susceptible-Infected-Susceptible (SIS) model proposed by Chen and Wei (2009). Theauthors use a new state Q of quarantined hosts. This model is called Susceptible-Infected-Quarantined-Susceptible (SIQS) model and allows the decision makers to isolate an infected host based on a previously determined rate of quarantine q. Adding a new state P of patched hosts, the conceptual design is modified to include the patched state and becomes susceptible-patched-infected-quarantined-susceptible (SPIQS) model (See Figure 1).

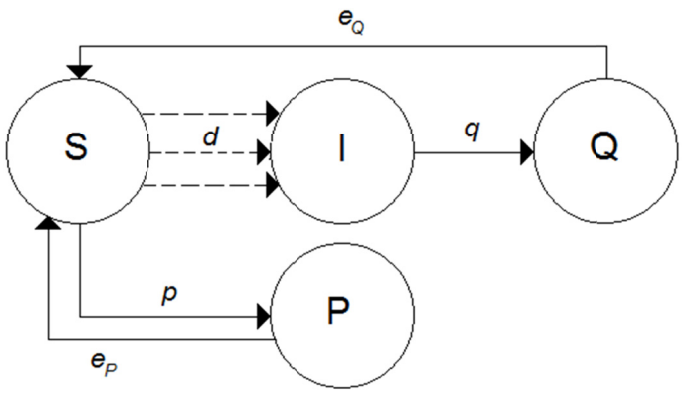

Figure 1. SPIQS model

When an infection arrives in a network with susceptible hosts, the spread of infection is based on several factors: number of hosts in the network (N), average infection time between two hosts (t), density of connections (d), degree of patching (p) before the infection arrives, and degree of quarantine (q) during the spread of the virus. While N represents the size of the network, t represents the time of virus reproduction, that is, the average time it takes for one host to infect another host. Density of connections d indicates the number of contacts that an infected host has during time t. When $d=0\%$, for example, an infected host has no contacts with the rest of the network during the time t, when $d=100\%$, an infected host is connected with all other hosts during the reproduction time. Also, degree of patching before infection arrives (p) and degree of quarantine (q) during the spread of virus can have values in the *0-100%* range.

The above mentioned input variables (N, t, d, p, and q) serve as the basis for creating the base and alternative scenarios during the simulation analysis. In addition, effective rate of patching (e_P) indicates the probability that a patched host is still susceptible due to the efficacy of antivirus program or the strength of the virus itself. Similarly, effective rate of quarantine (e_Q) indicates the likelihood that a quarantined host can become susceptible. The decision maker is prompted for these variables at the start of simulation model. The values used in the base simulation model are shown in Table 1.

Table 1. Main input variables used for the base scenario

Variable Name	Notation	Initial Value
Number of Hosts in the Network	N	1000
Average Reproduction Time	t	3 minutes
Connection Density	d	5%
Degree of Patching	p	30%
Degree of Quarantine	q	30%
Effective Rate of Patching	e_P	10%
Effective Rate of Quarantine	e_Q	5%

Once the base model is defined, alternative scenarios can be created by simply changing the values of the input variables. For example, when p=0% then a scenario with no patching (SIQS) is created. Similarly, when q=0% then a scenario with no quarantine (SIPS) is created. Alternatively, the impact of patching and quarantine into the total number of infected hosts can be investigated by creating scenarios with varying values of p and q respectively.

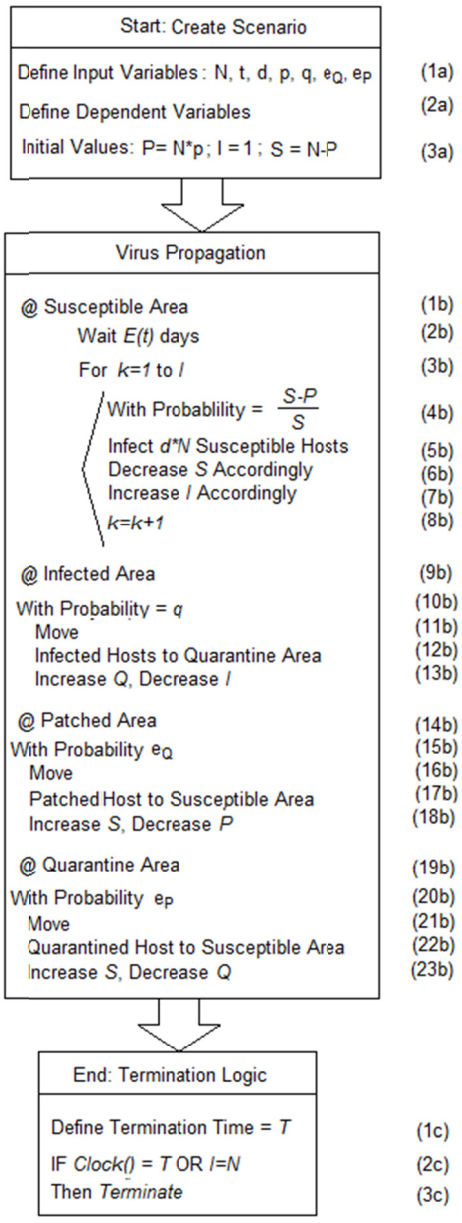

Figure 2. Simulation algorithm

Figure 2 shows high level algorithm for the proposed simulation model. As shown, there are three major components of the algorithm: a) creating a scenario, b) virus propagation, and c) model termination. The model starts with setting up the simulation scenario by defining input variables and calculating dependent variables. Note in line (3a) that *I=1*, which means that the simulation starts with only one single infected host. The main section of the algorithm is section (b) which takes place in four areas: @susceptible (lines 1b-8b), @infected (lines 9b-13b), @patched (lines 14b-18b), and @quarantine (lines 19b-23b). Once a virus has arrived and infected a host in the susceptible area, it will spread to other hosts. The time of reproduction is represented as exponential distribution *E(t)*. The virus will spread according to connection density *d* and with probability *(S-P)/S*. This probability represents the ratio between un-patched hosts and total number of susceptible hosts.

While the susceptible area can be used to investigate a patching strategy, the infected area can be used to investigate a quarantine strategy. Once infected hosts "arrive" at the infected area, some of them are moved to the quarantine area according to the quarantine strategy *q*. The patched and quarantine areas simply hold algorithm which allow some patched and quarantine hosts to return to the susceptible area if they are in fact susceptible according to the effective patched and quarantine rates. Finally, the simulation run will terminate when simulation clock reaches a predetermined amount of time (1c) or if all hosts are infected (2c).

5. Simulation Model and Preliminary Results

After each scenario is created, the simulation is run using an appropriate number of replications allowing for statistically significant results. Harrell, Bateman, Gogg, and Mott (1995) provide an approach to computing the number of replications required to ascertain a selected degree of accuracy. In our example, each scenario is replicated 100 times to ensure data reliability. The data generated by the model can be further analyzed to fine tune the model and the resulting decisions. The impact of "herd immunity" in the number of infected hosts can provide insights about the model's construct and its validity. We compared two alternatives: scenario model with "herd immunity" and scenario model where "herd immunity," formula in line (4b) of the algorithm, is purposefully suppressed.

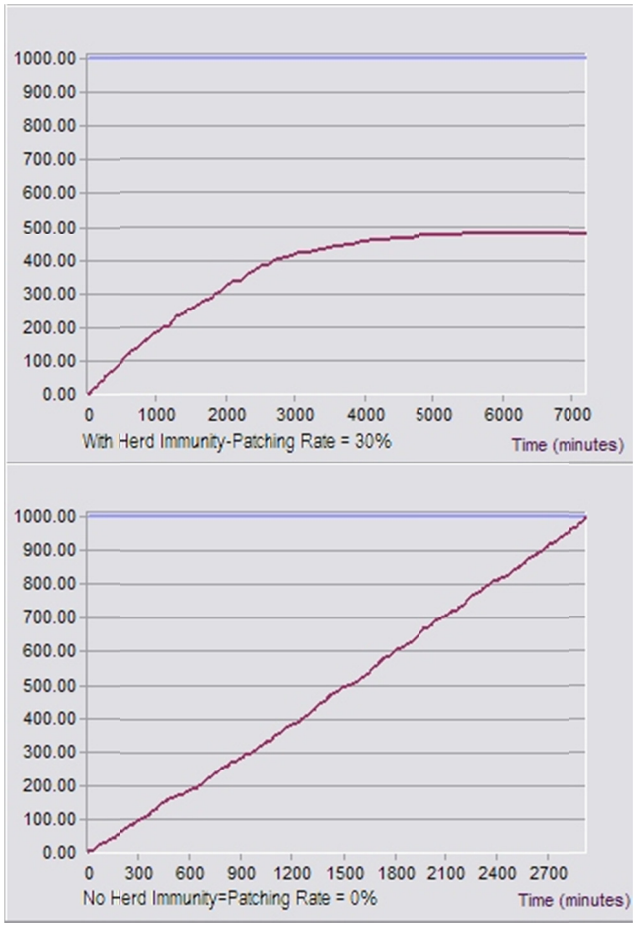

Figure 3. Infection over time

As shown in upper part of Figure 3, in a given scenario where the model is run for 120 hours and the patching rate is selected at 30%, the infection of the susceptible hosts in the network increases up to 480 hosts. Considering that about 300 hosts are already patched (30% patching rate) before the start of the attack, the model indicates that about 220 hosts are protected due to herd immunity. In fact, the number of hosts protected by herd immunity is higher, considering that patching is not completely effective. Our model, assumes that 10% of patched hosts (10% of 300 = 30 hosts) randomly return to a susceptible state, as such the number of hosts protected by herd immunity is 220+30 = 250. As a result, 25% of hosts in the network are protected by herd immunity.

The lower part of Figure 3, shows the spread of the virus when the herd immunity effect is purposefully suppressed (patching rate is 0%). As shown, all hosts in the network are infected within a short amount of time. It took only 48 hours and 48 minutes for the whole network to be infected. This analysis enforces the importance of the herd immunity effect and also re-enforces the validity of the model.

6. Impact of Patching Strategies

In an ideal situation, a network administrator would prefer to see no infection spread in the network. Theoretically, it seems that only way to reach this goal is to patch 100% of the hosts. Practically, this goal cannot be achieved because of several factors. First, even if the patching rate is 100%, there is no guarantee that the network will be completely protected. In the continuous battle between the virus creators and antivirus programmers, there are situations when the antivirus software is unable to protect every host in the network. Second, from a cost-benefit perspective, one may purposefully consider a patching rate of less than 100% to save on the costs and time of patching and hoping that herd immunity effect will protect the rest of the hosts. As a result, the expected damage to the network and to the business which runs on the network is not severe. Finally, implementing a patching strategy requires time and it is possible for the virus to spread at a faster rate than the rate of installing patching software throughout the network.

Under these circumstances, it would be more practical for the network administrator to set acceptable guidelines with regard to number of infected hosts and time to implement a patching strategy. In that situation, a decision must be made to identify an appropriate patching and quarantine strategy that meets those guidelines. For the sake of illustration, assume that 100 hosts are allowed to be infected and the herd immunity must start to take over as soon as possible. Simulation modeling can now be used to identify an appropriate patching and quarantine strategy which satisfies the above requirements. Specifically, the problem is formulated as follows: what is an acceptable patching and quarantine strategy that will not allow more than 100 hosts to be infected and that will bring the network into an endemic state at the shortest amount of time possible?

As shown in Figure 4, a 30% patching rate will ensure that no more than 500 hosts are infected; a 40% patching rate will ensure that no more than 300 hosts are infected; and a 50% patching rate will ensure that no more than 100 hosts are infected. As such, the simulation model indicates that *patching rate* has a significant impact on the resulting number of infected hosts. However, it seems that all of the above scenarios indicate the same amount of time (approximately 5000 minutes) required to place the network into an endemic state.

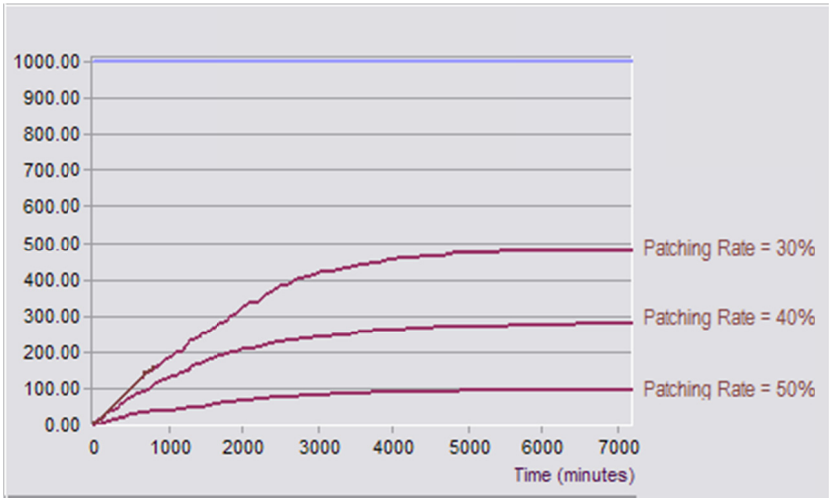

Figure 4. Virus propagation with different patching strategies

The simulation model is now adjusted to represent scenarios where hosts are not patched randomly. A patching strategy is followed where hosts with the highest average number of random connections are patched first. Specifically, two scenarios are compared: scenario d=5, where *connection density* is allowed to vary up to an average of 5 connections and scenario d=5, where *connection density* is allowed to vary up to an average of 3 connections. The second scenario assumes that hosts with average connections of 4 and 5 are patched at the start of the simulation run. As shown in Figure 5, the difference on the *connection density*has no significant impact on the resulting number of infected hosts. However, the *connection density* is shown to have a significant impact on the time when the spread of the infection in the network arrives at an endemic state (approximately 3000 minutes for *d=3* scenario versus 5000 minutes for *d=5* scenario).

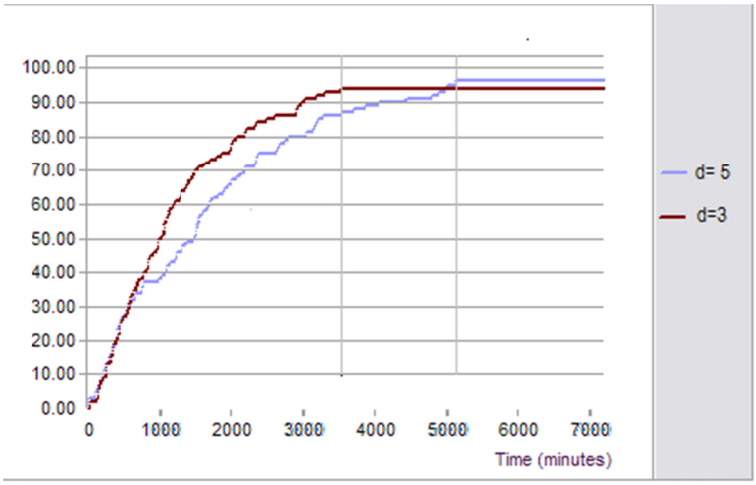

Figure 5. Virus propagation for scenarios with Different density

7. Impact of Quarantine Strategies

Besides patching, an effective quarantine strategy may have a significant impact on the number of hosts which are infected during a virus attack. Considering a patching rate of 50% as determined previously, simulation model is adjusted to create three additional scenarios: scenario *q=0%* where no infected hosts are quarantined, scenario *q=50%* where half of the infected hosts are quarantined and scenario *q=100%* where all of the infected hosts are quarantined.

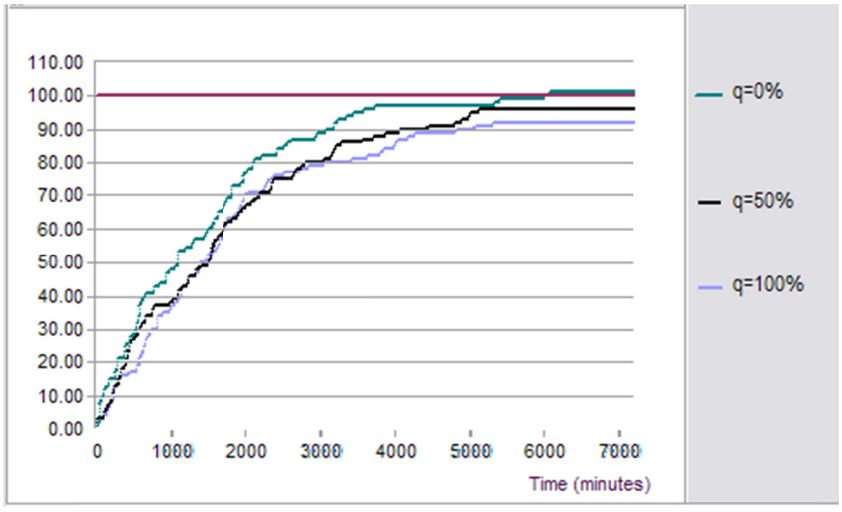

Figure 6. Virus propagation with 50% patching rate and different quarantine rates

Figure 6 indicates the number of infected hosts for the above three scenarios. Because the patching rate is 50%, it

expected that no more than 100 hosts are infected. Different quarantine rates provide no significant change in this number. The number of infected hosts varies from 92 to 100 even when the quarantine rate varies from 0% to 100%. Figure 6 also indicates no significant trend on reducing the time for the virus spread to reach the endemic state. It should be noted, that further investigation of the quarantine impact is needed. This investigation may include the impact of the quarantine rate for different patching scenarios and for non-homogenous networks.

8. Conclusions and Future Research

This paper proposes a simulation model which can be used as a decision making tool to formulate appropriate patching and quarantine strategies before and during a potential virus attack in a computer network. The model can be used by network administrators to identify appropriate responses using information about the network (number of hosts, connection density) and the expected virus (reproduction number, reproduction time and patching and quarantine effectiveness). The model can also be used to study the impact of herd immunity on the network given a selected patching strategy.

Simulation has several advantages over mathematical or other decision making methods. Simulation uses a logical abstraction of the reality through a computer model that "mimics" the behavior of the virus as it arrives in a given network target. Once the computer based simulation model is validated, the decision maker can test a range of alternative solutions for different scenarios. As such, the simulation model can be used to formulate appropriate response strategies against a network attack. The decision maker is able to evaluate IF-THEN scenarios, which would be difficult, if not impossible, to generate in the real environment.

The paper illustrates the use of the simulation model in the case of a homogenous network with 1000 hosts and a random connection density of approximately 5 percent. This network is attacked by a virus with an average reproduction time of 3 minutes. The simulation results indicate that patching is a far more efficient protection strategy than quarantine. In fact, patching seems to be the only strategy which utilizes the herd immunity effect to bring the spread on an endemic state. A carefully selected patching strategy, where the most active hosts are patched first, can lead to a significant reduction on the *time* required to bring the system in an endemic state.

As a final note, one should remember that a simulation model is only as good as the assumptions on which it is based. If a model makes predictions which are not supported by observed results, one must go back and change initial assumptions in order to make the model useful. The proposed model will serve as a basis for future studies where other factors can be incorporated. These factors include, but are not limited to, non-homogenous networks, costs of quarantine, costs of patching, and costs associated with loss of business due to infected computers. Further, the model can be extended to simulate different network configuration such as network size and structure.

References

Anderson, R. M., & May, R. M. (1991). *Infectious diseases of humans: Dynamics and Control*. New York, NY: Oxford University Press.

Anonymous. (2011). *Harvard Medical School*. Retrieved August 18, 2011, from http://www.health.harvard.edu/multimedia/herd-immunity-animation

Bailey, N. (1975). *The mathematical Theory of Infectious Diseases and its Applications* (2nd ed.). London: Griffin.

Chen, J., & Wei, S. (2009). Stability analysis of worm propagation dynamics based on quarantine. *2nd IEEE International Conference on Computer Science and Information Technology* (pp. 380 - 384). Beijing: IEEE. http://dx.doi.org/10.1109/ICCSIT.2009.5234704

Chen, T. M., & Jamil, N. J. (2006). Effectiveness of Quarantine in Worm Epidemics. *IEEE International Conference on Communications., 5*, pp. 2142-2147. Istanbul, Turkey: IEEE Press. http://dx.doi.org/10.1109/ICC.2006.255087

Christley, R. M., Pinchbeck, G. L., Bowers, R. G., Clancy, D., French, N. P., Bennett, R., & Turner, J. (2005). Infection in Social Networks: Using Network Analysis to Identify High-risk Individuals. *American Journal of Epidemiology, 162*(10), 1024-1031. http://dx.doi.org/10.1093/aje/kwi308

Cobb, C., & Myers, A. (2009). Antivirus Technology. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (5th ed., Vol. 1, pp. 41.1-41.14). Hoboken, New Jersey: John Wiley & Sons, Inc.

Diekmann, O., & Heesterbeek, J. A. (2000). *Mathematical Epidemiology of Infectious Diseases: Model Building,*

Analysis and Interpretation. New York, NY: Wiley Series in Mathematical and Computational Biology.

Fine, P. (1993). Herd Immunity: History, Theory, Practice. *Epidemiologic Reviews, 15*, 265-302.

Frauenthal, J. C. (1980). *Mathematical Modeling in Epidemiology*. New York: Springlerverlag. http://dx.doi.org/10.1007/978-3-642-67795-3

Garnett, G. (2005). Role of Herd Immunity in Determining the Effect of Vaccines Against Sexually Transmitted Disease. *The Journal of Infectious Diseases* , S97-S106. http://dx.doi.org/10.1086/425271

Geer, D. E., & Conway, D. G. (2009). Patch Grief with Proverbs. *Security & Privacy*, 86-87. http://dx.doi.org/10.1109/MSP.2009.164

Harrell, C., Bateman, R., Gogg, T., & Mott, J. (1995). *System Improvement Using Simulation* (3rd ed.). Orem, UT: PROMODEL® Corporation.

Hill, A. N., & Longini, I. M. (2003). The Critical Vaccination Fraction for Heterogeneous Epidemic Models. *Mathematical Biosciences, 181*, 85-106. http://dx.doi.org/10.1016/S0025-5564(02)00129-3

Kephart, J., & White, S. (1991). Directed-graph Epidemiological Models of Computer Viruses. *IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 343-359). Oakland. http://dx.doi.org/10.1109/RISP.1991.130801

Kermack, W., & McKendrick, A. (1927). A Contribution to the Mathematical Theory of Epidemics. *Proceeding of the Royal Society London, 115*(772), 700-721. http://dx.doi.org/10.1098/rspa.1927.0118

Kermack, W., & McKendrick, A. (1932). A Contribution to the Mathematical Theory of Epidemics: the Problem of Endemicity. *Proceeding of the Royal Society of London, 138*(834), 55-83. http://dx.doi.org/10.1098/rspa.1932.0171

Larson, R. C., & Nigmatulina, K. R. (2009). Engineering Responses to Pandemics. In *Information Knowledge Systems Management* (pp. 311-339). IOS Press.

McKendrick, A. G. (1925). Applications of Mathematics to Medical Problems. *Proceedings of the Edingurgh Mathematical Society*, *44*, 94-130. Edingburgh.

Mulligany, D. K., & Schneider, F. B. (2011). *Doctrine for Cybersecurity*. Retrieved August 17, 2011, from http://hdl.handle.net/1813/22739

Piqueira, J., de Vasconcelos, A., Gabriel, C., & Araujo, A. (2008). Dynamic Models for Computer Viruses. *Computer & Security* (pp. 355-359). Amsterdam, Netherland: Elsevier Ltd. http://dx.doi.org/10.1016/j.cose.2008.07.006

Pastor-Satorras, R., & Vespignani, A. (2002). Epidemics and Immunization in Scale-free Networks. In S. Bornholdt, & H. Schuster (Eds.), *Handbook of Graphs and Networks: From the Genome to the Internet* (pp. 1-22). Berlin, Germany: Wiley-VCH.

Tao, L., Weng, H., & Zhu, Z. (2008). Modeling and Analyzing the Spread of Worms based on Quarantine. *Proceedings of the 27th Chinese Control Conference* (pp. 299-301). Kunming, Yunnan, China: IEEE Press. http://dx.doi.org/10.1109/CHICC.2008.4605158

Wang, F., Zhang, Y., Wang, C., Ma, J., & Moon, S. (2010). Stability Analysis of a SEIQV Epidemic Model for Rapid Spreading Worms. *Computer & Security* (pp.*410-418*). Amsterdam, Netherland: Elsevier Ltd. http://dx.doi.org/10.1016/j.cose.2009.10.002

Zou, C., Gong, W., & Towsley, D. (2003). Worm Propagation Modeling and Analysis Under Dynamic Quarantine Defense. *Proceedings of the 2003 ACM Workshop* (pp. 51-60). Washington, D. C.: ACM Press.