An SII Model for Tracking the Propagation of Modern Email Malware

[I]Bincy George, [II]Liji Jacob, [III]Dhanya P J
[I]M.Tech Student, [II,III]Asst. Professor
[I,II,III]Dept. of CSE, Mount Zion College of Engg., Kadammanitta, Pathanamthitta, India

Abstract

The basic service of the computer user is email, but the email malware poses security problems. Email malwares are propagated through email services. To analyze the propagation of the malware is used to block these malwares and it can help to develop new security techniques. Reinfection and self-start are the two new features of the model email malware when comparing it with earlier versions. This paper introduces an analytical model called SII model is used to analyze the propagation of these modern email malware. The proposed model introduces the spreading speed of the modern email malwares that are caused by reinfection and self-start.

Keywords
Security, Email malware, Propagation, SII model, Reinfection, Self- start

I. Introduction

Malicious software infiltrates a target system's hardware and software resources and wreaks havoc by accessing sensitive information, stealing identities or committing other illegal actions. While anti-virus, encryption, firewall and other security products offer protection, these software solutions can be neutralized by malware that's running at the same or higher privilege levels.

Computer security is providing physical protection to prevent theft of or damage to the hardware, to prevent theft of or damage to the information and to prevent disruption of service. Most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware. Computer security used in both secrecy and integrity, the closely related area termed denial of service. Denial of service can be defined as a temporary reduction in system performance, a system crash requiring manual restart, or a major crash with permanent loss of data. Although reliable operation of the computer is a serious concern in most cases, denial of service has not traditionally been a topic of computer security.

In this real world all computer users using the email services, but malicious attachment in the email is poses some security issues. The earlier versions email propagation has followed the same mode. If a trusted email is sent to the victim and if the victim is clicking on the malicious attachment, the system will be compromised. Then immediately the compromised computer will start to infect new target in the email address. By focusing the propagation of modern email malware we can reduce the prevalence and spreading speed of malwares. Early malwares like Melissa infect the user only once i.e. non-reinfection.

The earlier versions of malwares like Melissa in 1999 and Love Letter in 2000 checks whether the victim is infected before compromising that system. In this paper introduces the two new features of the modern email malwares, Reinfection and Self-start. Reinfection means that the compromised system will reinfect whenever he/she clicking on malicious link. Self-start means that the malware copies send out from an infected user when ever some events triggered. The proposed system to develop a new analytical model that can precisely present the propagation dynamics of the modern email malware.The proposed model can precisely present the repetitious spreading process caused by reinfection and self-start and effectively overcome the associated computational challenges.

II. Literature Survey

A. Modelling and Simulation Study of the Propagation and Defences of Internet Email Worm

(Cliff C. Zou, Don Towsley, Weibo Gong) : says that as many people rely on email communications for business and everyday life, Internet email worms constitute one of the major security threats for our society. Unlike scanning worms such as Code Red or Slammer, email worms spread over a logical network defined by email address relationship, making traditional epidemic models invalid for modelling the propagation of email worms. In addition, we show that the topological epidemic models presented in [1], largely overestimate epidemic spreading speed in topological networks due to their implicit homogeneous mixing assumption. For this reason, we rely on simulations to study email worm propagation in this paper. We present an email worm simulation model that accounts for the behaviours of email users, including email checking time and the probability of opening an email attachment.

B. Spatial-temporal modelling of malware propagation in networks

(Zesheng Chen, ChuanyiJi) : says that on modeling the spread of topological malwares, which is important for understanding their potential damages, and for developing countermeasures to protect the network infrastructure. Our model is motivated by probabilistic graphs, which have been widely investigated in machine learning. We first use a graphical representation to abstract the propagation of malwares that employ different scanning methods. We then use a spatial-temporal random process to describe the statistical dependence of malware propagation in arbitrary topologies. As the spatial dependence is particularly difficult to characterize, the problem becomes how to use simple (i.e., biased) models to approximate the spatially dependent process. In particular, we propose the independent model and the Markov model as simple approximations.

C. Network Immunization with Distributed Autonomy-Oriented Entities

(Chao Gao, Jiming Liu, Ning Zhong) : In this work, author have presented a distributed and feasible immunization strategy that is based on the ideas of autonomy-oriented computing (AOC). In order to investigate the efficiency of our strategy, we have compared our strategy with some existing strategies using both synthetic and real networks, including those with community structures. Our experimental results have shown that the AOC-based strategy is effective for large-scale decentralized and community-based networks, and the robustness of the AOC-based strategy in dynamically evolving networks has been discussed in. Specially, the AOC-based strategy has the ability to scale up its computation based on the design of self-organization. The efficiency of our strategy will improve with the increase of network scale. The results have shown that the cost of the AOC-based strategy is lower than others.

To model the epidemic spreading on topological networks, early researchers adopt differential equations to present the propagation dynamics of malware. Their simulation models avoid the "homogeneous mixing" problem but cannot provide analytical propagation studies. Also there are some works which characterize the propagation dynamics of isomorphic malware, such as P2P malware, mobile malware and malware on online social networks. The main two disadvantages of the existing system are previous studies say that a user can be infected and send out malware copies only once, no matter whether or not the user visits a malicious hyperlink or attachment again and previous works did not take the two new features (reinfection and self-start) into account, and hence, cannot accurately estimate the propagation of modern email malware.

III. Proposed System

In this paper, propose a new analytical model to capture the interactions among the infected email users by a set of difference equations, which together describe the overall propagation of the modern email malware. Then we introduce a new concept of virtual nodes to address the underestimation in previous work, which can represent the situation of a user sending out one more round of malware copies each time this user gets infected. The perform result of empirical and theoretical study to investigate why and how the proposed SII model is superior to existing models.

A. System Architecture

The fig.1 shows the overall architecture of the proposed system.

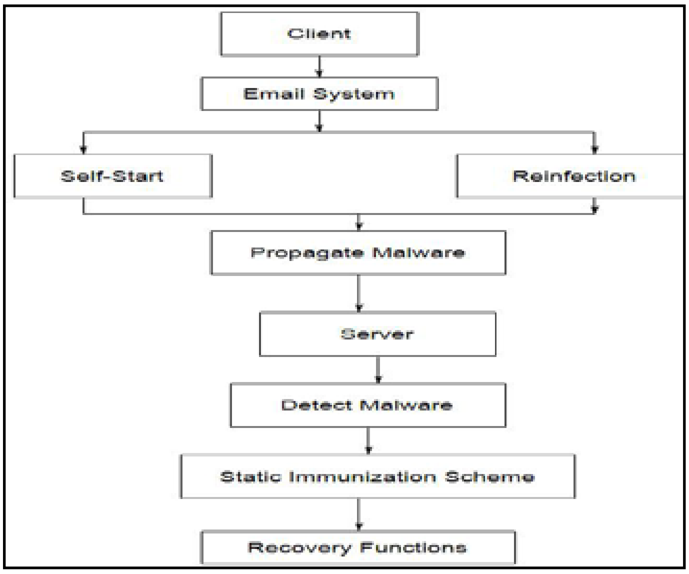


Fig. 1: Block diagram

B. Module Description

The main modules used in this work are

- Virtual Node Generation
- SII Model Creation
- Propagation Dynamics

1. Virtual Node Generation

The basic elements for the propagation of modern email malware are nodes and topology information. A node in the topology represents a user in the email network.The Virtual nodes, which can represent the situation of a user sending out one more round of malware copies whenever this user gets infected.For modern email malware, recall that a compromised user may send out malware email copies to neighbours every time the user visits those malware hyperlinks. Malware emails are also sent out when certain events are triggered. Thus, at an arbitrary time t,a user may receive multiple malware email copies from an identical neighbouring user who has been compromised. To represent the repetitious spreading process of there infection and the self-start, we introduce virtual nodes to present the kth infection caused by infected users whenever opening the k th malware email copy.

2. SII Model Creation

A node in the topology represents a user in the email network . Let random variable Xi(t) denote the state of a node i at discrete time t. Then, we have

$$X_i(t) = \begin{cases} \textbf{\textit{Hea.}}, \textit{healthy} \begin{cases} \textbf{\textit{Sus.}}, & \textit{susceptible} \\ \textbf{\textit{Imm.}}, & \textit{immunized} \end{cases} \\ \textbf{\textit{Inf.}}, \textit{infected} \begin{cases} \textbf{\textit{Act.}}, & \textit{active} \\ \textbf{\textit{Dor.}}, & \textit{dormant.} \end{cases} \end{cases}$$

In SII Model, use an M by M square matrix with elements pij to describe a topology consisting of M nodes, as in

$$\begin{pmatrix} p_{11} & \cdots & p_{1M} \\ \vdots & p_{ij} & \vdots \\ p_{M1} & \cdots & p_{MM} \end{pmatrix} p_{ij} \in [0,1],$$

where in pij represents the probability of user j visiting a deceptive malware email received from user i. If pij is equal to zero, it means the email address of user j is not in the contact list of user i. Therefore, the matrix reflects the topology of an email network. In this model, we assume the states of neighbouring nodes are independent. The infection of email malware depends on unwary email users checking new emails and visiting those malicious ones. An email user may receive multiple emails at different time, but read all of them at one time when the user checks the mailbox.

3. Propagation Dynamics

To represent the spreading process of virtual nodes, we extend Ni (the set of neighboring nodes of node i) into a new set of neighbouring nodes, Hi, which contains three subsets: Ni/N, Ni/R and Ni/S. First, the subset Ni/N includes the real neighboring nodes of user i. The nodes in Ni/N represent the neighboring users who visit the first malware email copy and get infected. Since the states of neighboring nodes are independent, each node is infected by neighboring nodes regardless of the state of this node. Second, the subset Ni/S includes the virtual nodes which present the extra spreading processes caused by certain events triggered in infected nodes. Third, the subset Ni/R includes the virtual nodes which present the extra spreading processes caused by users visiting more than one malware copies when they check new emails.

There are three preconditions for an arbitrary user being infected by email malware:

1. The user has not been immunized;
2. The user checks mailbox for new emails;
3. The user unwarily visits one received malware emails.

IV. Methodology

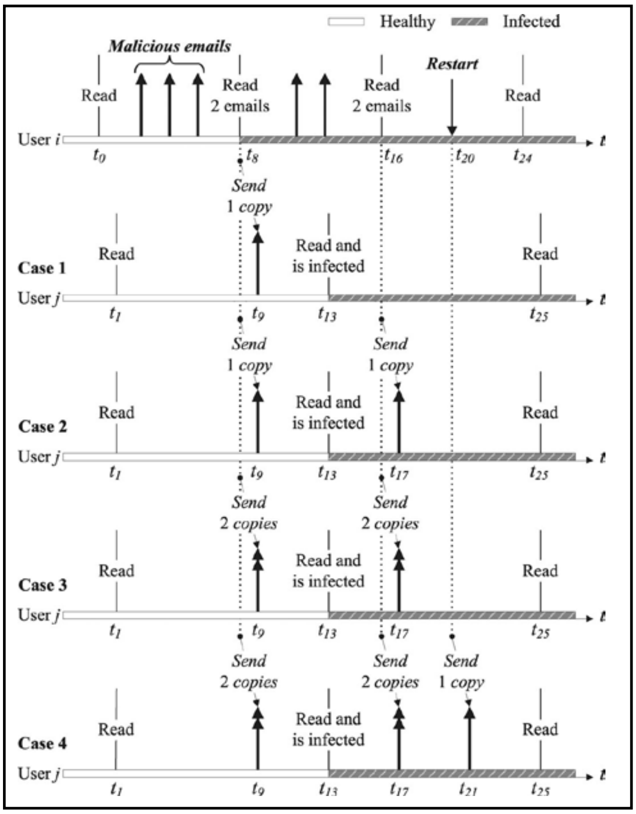
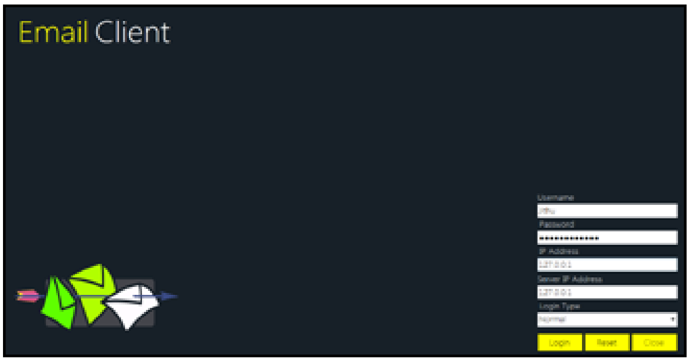


Fig. 2: Methodology

Suppose an email user i gets infected and sends out malware email copies to another email user j. In case 1 of the nonreinfection, although user i reads two malware emails at t, the user will get infected and send only one malware copy to user j at t8. The malware email arrives at user j at t9. Then, when user j checks mailbox at t13 and reads the malware email from user i, user j gets infected. User j will not receive any more malware emails from user i after t9. Nevertheless, in case 3 of the reinfection, user j will receive two malware copies from user i at t9. Furthermore, after user j gets infected at t13, when user i reads another two malware emails, user j receives another two malware copies from user i at t17. Compared with case 1 of the nonreinfection, user j in case 3 of the reinfection receives totally four malware emails.

V. Result Analysis and Performance Evaluation


Email Client

Username
jithu
Password
●●●●●●●●●●●●
IP Address
127.0.0.1
Server IP Address
127.0.0.1
Login Type
Normal

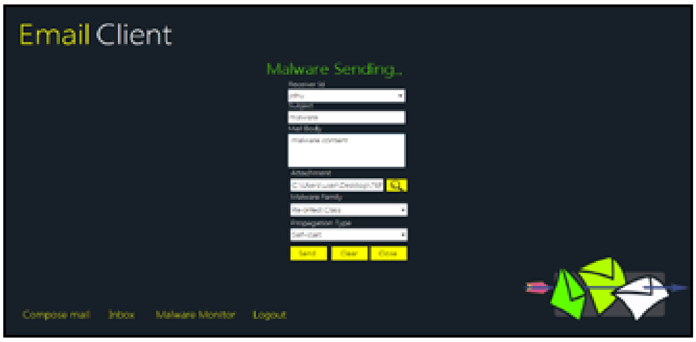
Fig. 3: Login page

Login Page is used to authenticate users. We can login only when server is available. When server active it broadcasts it's IP Address. Only after server IP Address is available Login button is active. User sends its username, password and login type to server, Server authenticates the user. Login type is used to determine the type of usage. There are two modes: attacker mode and normal mode.

Email Client

Fig. 4: Home page

In Home page we have links for compose mail, Mail Inbox, Malware Monitor and Logout. When we click Compose mail it checks the mode of login. If user has logged in normal mode, normal mail sending form is shown. If user has logged in attack mode , malware sending form is shown.

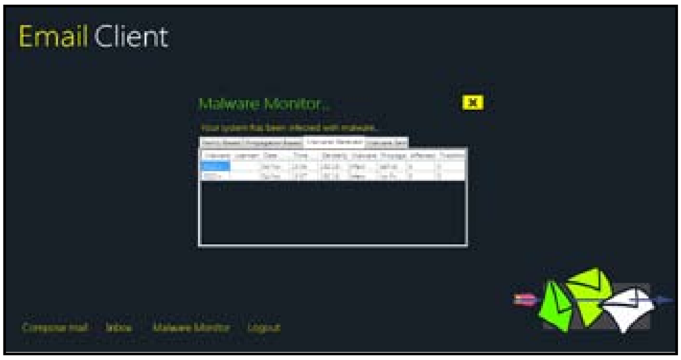

Email Client

Malware Sending..

Receiver Id
jithu
Subject
malware
Mail Body
malware content
Attachment
C:\Users\user\Desktop\?
Malware Family
Re-infect Class
Propagation Type
Self-start

Fig. 5: Attacker mail sending

This form is used to send malware content. First we should select the recipient and then attach the malware. Specify the Malware family. There are mainly two types of malware family based on there infection style. They are "Infect only" and "Re-infect"."Infect only" as its name specified infects user once only. If the user is attacked by the same malware once it will not infect it again. Re-infect type malware are more dangerous. It infects again and again. Specify the propagation type. There are two main types of propagation "Manual" and "Self start". "Manual" type malwares needs to send to another user like other mails "Self start" type malwares spreads itself based on system events.


Email Client

Malware Monitor..

Your system has been infected with malware..

Fig. 6: Malware monitor

It monitors the malwares that has attacked the users. It classifies and lists out the malware based on Malware family and propagation style.

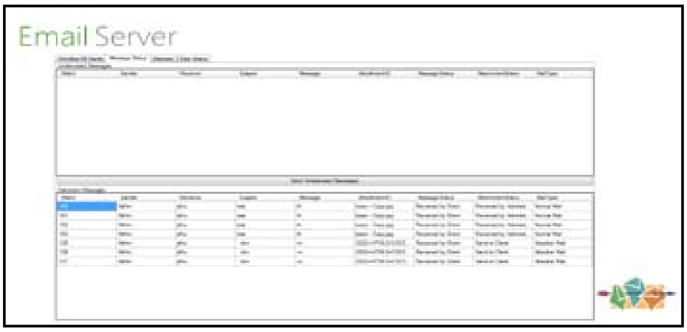


Fig. 7: Server side message status

It monitors the messages of clients. If the client is not active when a mail sent for him, the server saves the message and sends to him. Undelivered messages are shown in the above table. When we click the button "Send undelivered messages" the server checks the recipients of undelivered messages, it looks which all users are active. It forwards the mail to active users and keep the remaining mails.

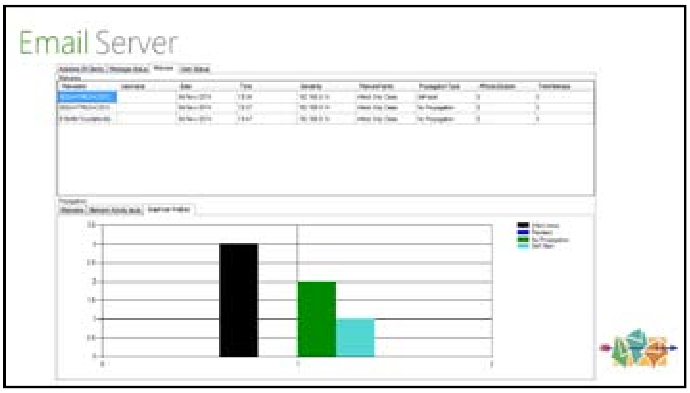


Fig. 8: Graphical analysis

It monitors and classifies the malwares based on their families and propagation styles. The classified data is graphically shown in fig.8.

VI. Conclusion and Futurework

In this paper, proposed an SII model for the propagation of modern email malware. This model is able to address two critical processes such as reinfection and self-start that is unsolved in the previous models. By introducing virtual nodes, we presented the repetitious spreading processes caused by the reinfection and the self-start. For the future work, there are also some problems needed to be solved, such as the independent assumption between users in the network and the periodic assumption of email checking time of users. The detectors analyze malware behaviors continuously and try to resist these techniques and strategies hence, we need to allow detection development techniques to lead malware updating through very well analytical process for malware activities and behaviors to fix any possible targeted threats. A new simulation must be designed to contain real system samples, to analyze the malware behaviors against these samples after elaborate malware updating. The objectives of this simulation are to avoid systems threats before being infected by real malware.

VII. AcknowledgEment

We would like to acknowledge the contribution of all the people who have helped in reviewing this paper. We would like to give sincere thanks to Mr. Anoop Chandran and Mr. Jithin James for there guidance and support throughout this paper. We would also like to thank our families and friends who supported us in the course of writing this paper.

References

[1] *M. Fossi and J. Blackbird, "Symantec Internet Security Threat Report 2010," technical report Symantec Corporation, Mar. 2011.*

[2] *P. Wood and G. Egan, "Symantec Internet Security Threat Report 2011," technical report, Symantec Corporation, Apr. 2012.*

[3] *C.C. Zou, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105- 118, Apr.-June 2007.*

[4] *Z. Chen and C. Ji, "Spatial-Temporal Modeling of Malware Propagation in Networks," IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1291-1303, Sept. 2005.*

[5] *C. Gao, J. Liu, and N. Zhong, "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," Knowledge and Information Systems, vol. 27, pp. 253-279, 2011.*

[6] *S. Wen, W. Zhou, Y. Wang, W. Zhou, and Y. Xiang, "Locating Defense Positions for Thwarting the Propagation of Topological Worms," IEEE Comm. Letters, vol. 16, no. 4, pp. 560-563, Apr. 2012.*

[7] *J. Xiong, "Act: Attachment Chain Tracing Scheme for Email Virus Detection and Control," Proc. ACM Workshop Rapid Malcode(WORM '04), pp. 11-22, 2004.*

[8] *S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling Propagation Dynamics of Social Network Worms," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 8, pp. 1633- 1643, Aug. 2013.*

[9] *(1999) Cert, advisory ca-1999-04, Melissa Macro Virus, http:// www.cert.org/advisories/CA-1999-04.html, 2009.*

[10] *Cert, Advisory ca-2000-04, Love Letter Worm, http://www.cert. org/advisories/CA-2000-04.html, 2000.*

[11] *M. Calzarossa and E. Gelenbe, Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures. Springer-Verlag, 2004.*

[12] *G. Serazzi and S. Zanero, "Computer Virus Propagation Models," Proc. 11th IEEE/ACM Int'l Conf. Modeling, Analysis and Simulations of Computer and Telecomm. Systems (MASCOTS '03), pp. 1-10, Oct. 2003.*

[13] *B. Rozenberg, E. Gudes, and Y. Elovici, "SISR: A New Model for Epidemic Spreading of Electronic Threats," Proc. 12th Int'l Conf. Information Security, pp. 242-249, 2009.*

[14] *(2001) Cert, Advisory ca-2001-22, w32/sircam Malicious Code, http://www.cert.org/advisories/CA-2001-22.html, 2001.*

[15] *Cert, Incident Note in-2003-03, w32/sobig.f Worm, http:// www.cert.org/incidentnotes/IN-2003-03.html, 2003.*

[16] *C. Wong, S. Bielski, J.M. McCune, and C. Wang, "A Study of Mass-Mailing Worms," Proc. ACM Workshop Rapid Malcode(WORM '04), pp. 1-10, 2004.*

[17] *D. Moore and C. Shannon, "The Nyxem Email Virus: Analysisand Inferences," technical report, CAIDA, Feb. 2006.*

[18] Symantec, A-Z Listing of Threats and Risks, http://www.symantec.com/security Response, 2012.

[19] C. Zou, Internet Email Worm Propagation Simulator, http://www.cs.ucf.edu/czou/research/emailWormSimulationhtml, 2005.

[20] M. Boguna, R. Pastor-Satorras, and A. Vespignani, "Epidemic Spreading in Complex Networks with Degree Correlations," Lecture Notes in Physics, vol. 625, pp. 1-23, 2003.

[21] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, "Epidemic Spreading in Real Networks: An Eigenvalue Viewpoint," Proc. 22nd Int'l Symp. Reliable Distributed Systems (SRDS), pp. 25-34,

[22] A.J. Ganesh, L. Massouli, and D.F. Towsley, "The Effect of Network Topology on the Spread of Epidemics," Proc. IEEE INFOCOM '05, pp. 1455-1466, 2005.

[23] D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin, and M. Faloutsos, "Information Survival Threshold in Sensor and p2p Networks," Proc. IEEE INFOCOM '07, pp. 1316-1324, 2007.

[24] Y. Wang, S. Wen, S. Cesare, W. Zhou, and Y. Xiang, "Eliminating Errors in Worm Propagation Models," IEEE Comm. Letters, vol. 15, no. 9, pp. 1022-1024, Sept. 2011.

[25] H. Ebel, L.I. Mielsch, and S. Bornholdt, "Scale-Free Topology of Email Networks," Physical Rev. E, vol. 66, no. 3, Sept. 2002.

[26] M.E. . Newman, S. Forrest, and J. Balthrop, "Email Networks and the Spread of Computer Viruses," Physical Rev. E, vol. 66, no. 3, 2002.

[27] T. Bu and D.F. Towsley, "On Distinguishing between Internet Power Law Topology Generators," Proc. IEEE INFOCOM '02, pp. 638-647, 2002.

[28] G. Yan, G. Chen, S. Eidenbenz, and N. Li, "Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications," Proc. Sixth ACM Symp. Information, Computer and Comm. Security (ASIACCS '11),, pp. 196-206, 2011.

[29] W. Fan and K.H. Yeung, "Online Social Networks-Paradise of Computer Viruses," Physica A: Statistical Mechanics and Its Applications, vol. 390, no. 2, pp. 189-197, 2011.

[30] S. Wen, "Topology Generator and Propagation Simulator of Modern Email Malware," Experement Result, http://www.deakin.edu.au/wsheng/emailpropagation.html, 2012.

[31] G. Eschelbeck, "The Laws of Vulnerabilities," Proc. BlackHat Conf., 2004.

[32] R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale-Free Networks," Physical Rev. Letters, vol. 86, pp. 3200-3203, 2001.

[33] R. Thommes and M. Coates, "Epidemiological Modelling of Peerto- Peer Viruses and Pollution," Proc. IEEE INFOCOM '06, pp. 1- 12, 2006.

[34] Y. Moreno, J.B. Gomez, and A.F. Pacheco, "Epidemic Incidence in Correlated Complex Networks," Physical Rev. E, vol. 68, Sept. 2003.

[35] D.H. Johnson and S. Sinanovic, "Symmetrizing the KullbackleiblerDistance," technical report, Rice Univ., Houston, TX, 2001.

[36] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms (Extended Version)," IEEE Trans. Mobile Computing, vol. 8, no. 3, pp. 353-368, Mar. 2009.

[37] S.M. Cheng, W.C. Ao, P.Y. Chen, and K.C. Chen, "On Modeling Malware Propagation in Generalized Social Networks," IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.