NETWORK SIZE, DETERRENCE EFFECTS, AND INTERNET ATTACK INCIDENT GROWTH

KALLOL KUMAR BAGCHI, University of Texas at El Paso
Dept. of Information & Decision Sciences, El Paso, TX 79968-0544, E-mail: kbagchi@utep.edu

ZAIYONG TANG, Louisiana Tech University
Department of Management and Information Systems, College of Administration and Business, Ruston, LA 71272, E-mail: ztang@cab.latech.edu

ABSTRACT

This paper introduces size-adjusted growth models of network security attacks. The primary aim of this article is to test the hypothesis that rapid growth of network attack incidents is at least partly explainable by the exponential increase in network size. The growth of network security attacks is modeled from information obtained after looking into: (i) imitation and deterrence processes involved in an attack, and (ii) how network externalities such as size influence the growth process. The non-linear models are estimated by using data from network security attacks obtained during the course of 10 years. We first show that network size is strongly correlated with various types of attack incidents, thus lending proof that size is an important factor in most network security attacks. Next, the results obtained from the diffusion models show that when both imitation and deterrence activities are taken into account and size effect is also added to a growth model, the attacks can be modeled more realistically. The targeted audience of this paper are IS researchers and professionals with interest in IS security.

INTRODUCTION

The number of security attacks is growing rapidly. In the first three quarters of 2002, the number of reported global security incidents rose to 73,359, which far surpassed the total 52,658 reported incidents in 2001. Recently, a deadly worm named Blaster hit at least 330,000 machines around the world and caused damage to the tune of more than $320 million as of August 2003 (Messmer 2003). Nodes or stations on the Internet and websites
are regularly attacked and the number of break-ins or attempted break-ins is steadily on the rise. Internet attack types include denial of service (DOS), worm and virus, domain name system (DNS) attack, router attacks, and web defacement (Denning 2000). The 2002 CSI/FBI report discusses many other types of computer- and Internet-based attacks or misuses such as financial and telecom fraud, telecom eavesdropping, sabotage, laptop misuse, active wiretap, and insider abuse of net access to name a few (Power 2002). The combined effect of all these attacks is devastating at times. One needs to find out how the attacks are growing and what factors are fueling such rapid attack growth.

One of the important contributors to the growth of such attacks is the size of the network. The growth of the Internet/the Web is phenomenal. Internet traffic, which was growing at a rate of 100% per year in the U.S., was expected to overtake telephone traffic in the U.S. by the end of 2003 (Coffman and Odlyzko 1998). Rai, Ravichandran, and Samaddar (1997) observed that the growth of the Internet is exponential in nature and that traditional contagion models fail to explain the growth.

Although network size can be an important factor in attack growths, this fact needs to be empirically tested. This article addresses the growth of security attacks with the help of exponential size-adjusted non-linear diffusion models. To test the hypothesis, we use the data on Internet security attacks from CERT/CC and the network size data from the World Bank. Our results show the impact of network size on the number of security attacks.

We use the growth theory, security theory, and network externality theory in this study. Standard growth or diffusion theory can explain the growth of a technology or a phenomenon of interest (Mahajan and Peterson 1987). Traditional logistic and Gompertz models (depending on different assumptions of the nature of growth) can explain how a product or a phenomenon is diffused over time, based on the word-of-mouth propagation. Traditional diffusion

**CONTRIBUTIONS**

Since the inception of the Internet, security attack incidents have increased rapidly. These attacks have caused enormous financial damage to industry, government, and society in general. For example, the reported annual losses due to attacks in the year 2003 amounted to $201,797,340 (Richardson 2003). Network exponential size effect is considered in the diffusion models of the Internet attack incidents that lead to a better prediction of the number of network attack incidents. We test the hypothesis using Internet attack incident data from Computer Emergency Response Team Coordination Center (CERT/CC 2001) and using a measure of Internet size represented by the number of Internet users per 1,000 people, obtained from the World Bank.

Additionally, by modeling the attack incident growths as a combination of attacks and deterrence schemes, the modeling framework as adopted in the paper encompasses a more realistic picture of attack growths (Bagchi and Udo 2003).

The study provides preliminary empirical evidence that network size matters in predicting Internet attack incident growth. Diffusion models designed by incorporating size can better predict the attack incident growth. There is a strong correlation between Internet size and various attack incident numbers.

Security is an important topic in information systems management and recently research interests have been focused on this topic (Brancheau, Janz, and Wetherbe 1996), (Householder, Houle and Daughtery 2002), (Micksch 2000), (Watson, Kelly, Galliers and Brancheau 1997). This research should be of interest to researchers who deal with the economic impact of Internet attacks. This research is also expected to be of moderate interest to all Information Systems (IS) researchers, practitioners, policy makers and managers who have to deal with the ever-increasing Internet security concern. Practitioners can also benefit from this research by noting the added impact that size has on the growth of Internet attacks.
models are used to model mostly good innovations; a change in modeling assumptions is needed to model the attack incident growth because such a growth depends on imitative behaviors as well as preventive mechanisms employed over time as noted by some scholars (Pitcher, Hamblin and Miller 1978), (Straub 1990), (Straub and Welke 1998). We also use network externality theory in our model. Network externality has been defined as a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes (Farrell and Saloner, 1985). Take the example of the Internet. Users of the Internet can interact with other users. Thus, an increase in Internet size can create more values for the Internet. That may explain why more Internet attacks are taking place. These theories together can better explain the attack growth incidents, as will be shown in this article.

The paper consists of seven sections. Section 2 provides background on network externality theory. In section 3 we explain the growth or diffusion theories and proposed models. Section 4 discusses the impact of different externalities. Section 5 deals with the data used, presents the results of regressions, and explores. Section 6 provides a summary of results, and section 7 (conclusions) presents the interpretation of results and suggestions for further research.

THE NETWORK EXTERNALITY THEORY AND THE ROLE OF SIZE

The Network Externality theory (Arthur 1989), (David 1985), (Farrell and Saloner 1985), (Katz and Shapiro 1986), (Varian 2001), (Windrum and Swann 1999) states that the value of a network depends on, among other things, the number of its nodes (i.e., size of the network), assuming full connectivity. Other researchers of network externality theory emphasize the relationship between the value of a network and the network content (Asvanund, Clay, Krishnan, and Smith 2002). Negative network externalities are also considered in research. For example, in an EDI context, positive externalities for buyers are generated when more suppliers join in; however, this also generates negative externalities for the suppliers (Wang and Seidmann 1995). This paper deals with positive network externality in the form of network size as it is incorporated in diffusion models.

One problem is determining the functional relationship between the size of a network and the network’s value. Three assumptions on these relationships exist (Gottinger 2000): linear, logarithmic, and exponential.

- Linear: as networks grow, the marginal value of new nodes is constant.
- Logarithmic: as networks grow, the marginal value of new nodes diminishes, network externalities at the limit are inconsequential, zero, or negative in comparison to quantifying effects on prices. Katz and Shapiro (1986) observed that network externalities are positive but diminish in value and at the limit are zero.
- Exponential: as networks grow, the marginal value of new nodes increases. An example of this is the Metcalfe’s law (Metcalfe 1995). Metcalfe’s law states that the value of a network is proportional to the square of the number of its users.

One can also combine these three assumptions in some fashion. Thus, a combination of Metcalfe’s law and logarithmic assumption can lead to an S-curve-like function (Rogers 2003). The assumption is that while early growth is exponential, later additions diminish in their marginal value. Another combination possibility could be that in later stages of adoption, the size contributes in an exponential manner. Thus, instead of growth diminishing as per an S-curve, the growth continues unabated. This is the argument made in this paper as network security attacks are studied.

The value of the Internet to attackers is an important aspect in generation of such attacks. With the increase in number of attacks, the value of the Internet to the attackers also increases. Future attackers find the system more and more attractive to fashion an attack. Since anyone who can break a system gets “recognition” from other intruders, attackers usually have responded to this added value. Internet attacks generate universal and quick attention. Therefore, attackers devise newer ways to deface Web sites, introduce newer and
more destructive versions of viruses/worms, and generate distributed denial of service attacks. The question is: As the Internet grows in size, will the value in such attacks also grow, resulting in an exponential growth in attacks? An answer is attempted via the help of a few new models designed for this study. A few size-based extensions to pure diffusion models are introduced. We first consider a security attack model with S-curve-like features that assumes that the growth will reach a maximum limit at a certain point and then will decline. Extensions of this S-curve model with an exponential, linear and logarithmic parts are next considered, which assume that the attacks will show an exponential, linear or logarithmic growth in later stages as the size of the network continues to grow.

A COMBINED GROWTH THEORY AND SECURITY THEORY FRAMEWORK

Rogers (2003) notes that diffusion/growth theory studies are growing at the rate of 120 diffusion studies a year, and that no other behavioral science research is so extensive and well-grounded in theory. The growth theory assumes that growth curves are like S-curves, i.e., the natural growth rate starts slowly, gradually increases until it reaches an equilibrium level (called an inflection point), and then tapers off. Growth can also be induced by technological changes as the quality of the product improves and continuously raises the equilibrium level. Growth models can combine these two growth types.

One of the ways to incorporate the effect of technological changes in the natural growth process of a product is to assume that the equilibrium level of the growth curve is a function of price given quality (Gurbaxani and Mendelson 1990). However, for modeling network attack incidents, a better approach could be to assume that technological changes are increasing the size of the network. Thus the effect of size could be included in the natural growth model.

Finally, prior research has shown that growth of many innovations at least in the initial stages is more like an exponential one (Rogers 2003). One can similarly argue that attack incidents have also grown exponentially. Thus an exponential part can be added to a diffusion model to see if the growth of attack incidents follows such a model.

Growth analysis in terms of imitation and deterrence processes

Traditional growth models fail to analyze the security attack phenomenon adequately, as these are based on either a supply-demand rationale or on a learning perspective, or they use a technological substitution or use a communication theory based frame of reference (Mahajan and Peterson 1987). None of these frameworks is adequate for modeling security attack incident growth. Several other network security models exist. Operational models of network attack detection exist. Denning (1987) introduced an intrusion detection model that operated on audit record trail. Verwoerd and Hunt (2002) describe many intrusion detection techniques such as statistical models, neural networks, state transition analysis etc., for modeling normal and abnormal behaviors. Moitra and Konda (2004) examine reported network incidents over time. They observed that distribution of inter-attack times is exponential in nature and that the rate of attacks indicates an increasing trend. Shimeall and Williams (2001) describe a framework for conducting security trend analysis. Trending can be temporal, spatial, and associational depending on the situation encountered. A trend generation process establishes a baseline pattern for a trend and a detection of a change in the pattern indicates an abnormal situation. Instead of modeling attacks as a series of events, Templeton and Levitt (2000) consider attacks as a set of capabilities that provide support for abstract attack concepts. However, none of these studies describe or analyze attack incident growth in terms of imitation, deterrence and network size. Previous research has recognized the need to consider both deterrence and imitation of attacks in modeling the growth of network security attacks (Pitcher, Hamblin and Miller 1978), (Straub 1990).

Intuitively, implementing deterrence procedures and preventive measures would result in lower security attacks. This is partially supported by Straub’s (1990) empirical study, in which he found that computer abuse decreases when deterrence procedures and preventive security software were used. Increasing security awareness
Network Size, Deterrence Effects, and Internet Attack Incident Growth

through education and training also helps in reducing network security breaches (Straub and Welke 1998). Loch and Conger (1996) found that attitude and social norms are vital with respect to the intention of engaging in legal or illegal computing acts. Thus, a network security model should explicitly include the influence of deterrence and preventive procedures (Bagchi and Udo 2003). Our security attack growth model considers deterrence as well stimulus (e.g., imitation) together with size in explaining the growth process.

Behavioral aspects of network attacks

Imitative side: hackers and other attackers

One of the primary attack motivations is sociological: peer reinforcement. Bandura (1986) observed that people only engage in harmful attack incidents when they feel threatened and feel like acting by observing the successful aggression or attack done by earlier attackers. Thus every attack incident can be regarded as an imitation of previous behavior and a behavioral model for other attackers to follow. Hackers constitute a large section of people who creates such attacks. Hacker psychology varies to a great extent. According to some hacker experts, sometimes they just want to imitate or have fun. Many of them have a teenager-type mentality and they do it because their friends are doing it, and they want to achieve something by doing it (Kopytoff 2003).

Sometimes, hackers may generate these network attacks to protest against unfair dominance of the Internet by business. A “hacker ideology” may have become fashionable in young Internet users and it is possible that a significant minority of young users may view attacks as a legitimate and productive mode of protest against the dominance of the Internet by large corporations. Some experts also agree to this viewpoint (Kopytoff 2003), (Sinrod and Reilly 2000).

Another explanation of attacks could be that some of them are generated by young hackers to gain attention. Traditionally, the challenge for such attackers has been not criminal but an intellectual exercise to penetrate a system (Dreyfus 2002). In recent times, apart from pure hacking, different criminal intentions such as making money, taking economic and political advantages, etc., have emerged (Power 2002), (Turoff 2004). We discuss some of these issues below in more details. All of these issues are probably related to the size of the Internet—as the number of Internet users grow, these attacks types are also expected to grow.

Take for example, the economic incentives on the net. Some recent cases from the Department of Justice (US DOJ) illustrate the rapid rise of this kind of attacks (CCIPS 2004).

- In July, 2004, a Californian woman was charged with fraudulently using her computer to embezzle more than $875,035 from North Bay Health Care Group. The victim firm is a not-for-profit organization which operates hospitals and clinics in Vacaville and Fairfield, California.
- In May 2004, a Pennsylvania man was sentenced to prison for illegally accessing a Massachusetts Investor’s On-line investment account and making $46,000 in unauthorized trades.
- In November, 2003, three men were indicted for hacking into Lowe's Companies' Computers with intent to steal credit card information. According to Power (2002), the biggest financial fraud problem is the theft of large quantities of credit-card records from ill-protected servers.

Some firms/nations want to become information monopolies by destroying competitors. An example case cited in (Power 2002) will illustrate the point. In July 2001, a software firm called Avant was ordered to pay $182 million for stealing source code from Cadence, a competing firm.

Sometimes intelligence operations are encouraged by corporations and governments to gather information on competitors. Here are some recent cases:

- The CSI/FBI report of 2003 (Richardson 2003) cites the case of a person who left a firm named TBC to join a competitor of the firm in 2001. The man made several unauthorized accesses to TBC’s computer systems using his Internet connections to
gain a commercial advantage resulting in $21,636 in damages and costs to TBC.

• Two Chinese scientists and a U.S. citizen were charged with stealing the source code to Lucent Technologies PathStar for the Chinese firm Datang Telecom (Power 2002).

Geopolitical conflicts also contribute to attack incidents. The CSI/FBI report of 2002 indicates that a large percentage of web site defacements were due to geopolitical conflicts such as those that occurred in the Middle East, the Indian subcontinent and the Chinese populated regions. For example, China and Taiwan domain names constituted about 9% of all web site defacement incidents. Israel domain names registered a 220% increase in defacements. The corresponding % increase in defacement incidents for India and Pakistan was 205% and 300% respectively. Domains such as .mil and .gov registered a 128% and 37% increase in web site defacements during this period, thus indicating that U.S. government and military web sites were increasingly under the attack.

From a political point of view, no real effective international agreements in this area exist, although some efforts have been made in the recent past. Forty-one European countries, plus the U.S., Canada and Japan signed a treaty that supplies a legal framework aimed at the protection of society against cyber-crime (Convention 2001).

Cultural and institutional factors also come into play. Many poor foreign governments do not have the necessary work ethics at place or the infrastructure to prevent it. Finally, the lack of an adequate technology to prevent attacks is an important factor to consider. It is the individual users or firms who end up paying for the necessary protection costs which sometimes could be prohibitive.

We next discuss the deterrence side of the attacks such as legislative effects and the increase deployment of sophisticated security systems.

Deterrence side: legislative effects

Security laws and regulations of a nation aid the inhibition side of the equation. Compliance with law when properly enforced may inhibit security attacks. The U.S. government already has some laws and regulations in place related to computers, access devices, and communication lines, stations, and systems. The Computer Fraud and Abuse Statute of 1986 (USC 1030) states that anyone who knowingly or intentionally accesses a computer without authorization or exceeds authorized access is liable to be punished.

There are several laws that may act as a deterrent to hacking/cracking activities, as cogently articulated by Sinrod and Reilly (2000). These are summarized in Table 1.

The Patriot Act of 2001 made some relevant changes to the Computer Fraud and Abuse Act (CFAA) to make it stricter (Reilly 2002). The new by-laws include better anti-hacking provisions, a change in determining a hacker’s intent to cause a specified loss, implication for computers located outside the U.S., expansion of civil damages, and protection of hardware, software, and firmware firms.

To give an example, this statute makes it clear that an individual needs only to show intent to damage the computer or information on it and no specific dollar amount of loss or harm is required to convict an offender.

Deterrence side: other defensive acts

Another major deterrence effort has been in the direction of developing counter attack tools and frameworks such as anti-virus software, firewalls, etc. These tools are improving with the passage of time, making it increasingly difficult for an attacker to mount an offensive against the network (Bass 2000), (Jain, Hong and Pankanti 2000), (Schneier 1999), (Zviran and Haga 1999). However, with the release of each hardware and software, vulnerabilities do creep in, and intelligent attackers always find a way to attack the system by exploiting the vulnerabilities. Finally, some researchers (Alles et al. 2004) discuss the design of an emergency-preparedness system that can proactively deter many such attacks and can be considered as a system of the future.
Table 1. Summary of Internet Attack-related Laws

<table>
<thead>
<tr>
<th>Statute Name and Number</th>
<th>Where Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Computer Fraud and Abuse Statute of 1986 (USC 1030)</td>
<td>Knowingly or intentionally accessing a computer without authorization or in excess of authorized access</td>
</tr>
<tr>
<td>The USC $1029(a)(7)</td>
<td>Telecommunication instruments that have been modified or altered to obtain unauthorized use of telecommunication services</td>
</tr>
<tr>
<td>18 USC $1343</td>
<td>Prohibits intentional scheming to obtain money or property by means of false pretenses by wire</td>
</tr>
<tr>
<td>18 USC $1030(a)(3)</td>
<td>Criminalizes intentional access of non-public computers</td>
</tr>
<tr>
<td>18 USC $1030(a)(2)(c)</td>
<td>Criminalizes intentional access of information from a protected computer</td>
</tr>
<tr>
<td>18 USC $1030(a)(4)</td>
<td>Liable if obtained something of value more than $5,000</td>
</tr>
<tr>
<td>18 USC $1030(a)(5)</td>
<td>Liable if caused damage of value more than $5,000</td>
</tr>
<tr>
<td>15 USC $1644(b)</td>
<td>Liable if credit card number is transferred illegally over the phone</td>
</tr>
<tr>
<td>18 USC $1029(a)(2) or (3)</td>
<td>Liable if used unauthorized access device within a year and obtained anything of value &gt;$1,000</td>
</tr>
<tr>
<td>18 USC $1030(a)(5)(b)-(c)</td>
<td>Criminalizes intentional damage of a computer</td>
</tr>
</tbody>
</table>

Network attack growth models

Thus, imitation and inhibition as assumed by our proposed model combined with the size influence could provide a realistic background in modeling attack incidents. Two traditional growth models, the logistic model (S-curve based) and the exponential model, without the incorporation of the size impact are presented in Table 2. Also, the model used by Pitcher, Hamblin and Miller (1978) (hereafter called the PHM model in this paper) is used in this study and shown in Table 2, which assumes that the probable causes for outbreak of such attack incidents are imitative as well as inhibitive in nature and the growth is asymmetric in nature.

Network size-adjusted extended models

First, an extension (based on the size) of the PHM model is developed. The attack incident growth curve can be analyzed by examining the rate of logarithm of cumulative attack incident data (Gurbaxani and Mendelson 1990) given by:

\[ \frac{d\text{Attck}_t}{dt} = \log(\text{Attck}_t) - \log(\text{Attck}_{t-1}) \]  

(2)

For the yearly data, the discrete analog of (1) can be used which is:

\[ \frac{D\text{Attck}_t}{\text{Attck}_{t-1}} = \log(\text{Attck}_t) - \log(\text{Attck}_{t-1}) \]  

(3)

where \( K \) is the upper bound of growth.

Table 2. Formulation of Different Diffusion Models

<table>
<thead>
<tr>
<th>Model Type</th>
<th>Formulation of cumulative growth rate</th>
</tr>
</thead>
</table>
| *The Logistic Model* | \( \frac{d\text{Attck}(t)}{dt} = b\times\text{Attck}(t)\times(\text{Attck}\text{bar} - \text{Attck}(t)) \)  
At\text{ck}\text{bar} \( \rightarrow \) upper limit of cumulative incident attacks  
\( b \rightarrow \) rate of growth |
| *The Exponential Model* | \( \frac{d\text{Attck}(t)}{dt} = g \times \text{Attck}(t) \)  
g \( \rightarrow \) the growth rate constant |
| *The PHM Model* | \( \frac{d\text{Attck}(t)}{dt} = c \times e^{-q \times t} \times \text{Attck}(t) \)  
c \( \rightarrow \) the net rate of instigation to attacks and  
q \( \rightarrow \) the rate at which they are inhibited |
The formulation for $D_{\text{Attck}}$, for the logistic model is:

$$D_{\text{Attck}} = \log(b) \times [K \times (\text{Attck}) - 1]$$

For the data obtained from CERT/CC, the plot of $D_{\text{Attck}}$ over time $t$ is shown in Figure 1. It appears that $D_{\text{Attck}}$ decreases over time $t$ for sometime after which it becomes flat (with noise added). This slow down of $D_{\text{Attck}}$ may not be completely captured by a pure S-curve. The growth is more like an S-curve initially and later became exponential in nature. A single model that can capture this growth phenomenon should have both elements represented in the model. What can cause this exponential-like growth in later years? One of the factors that may explain such growth is the network size factor.

It is, therefore, hypothesized that a growth model incorporating a network size factor may adequately describe the growth process of attack incidents. In the following, the formulation with various size factors is shown.

Network externality theory assumes that the bigger the size of the network, the higher the value of a product that leads to more adoptions. The original security attack incident model can be represented mathematically as:

$$\frac{d\text{Attck}(t)}{dt} = c \times e^{-q \times t} \times \text{Attck}(t)$$

This results in $\text{Attck}(t)$ as an S-shaped curve. Now the nature of the growth series depends not only on the S-shaped curve $\text{Attck}(t)$, but also is a function ($g(\text{Int}_t)$) of the “size of the network” series represented by $\text{Int}_t$. Let us denote the new size-adjusted growth series as $S_{\text{Attck}}(t)$. Then

$$S_{\text{Attck}}(t) = \text{Attck}(t) \times g(\text{Int}_t)$$

**IMPACT OF DIFFERENT EXTERNALITIES**

Network externality in the form of size may influence the development of all types of
security breaches. As the Internet grows exponentially, security breaches may tend to grow in a similar fashion. As Power and other experts note, Internet-based attacks are steadily on the rise (Power 2002). The size of the Internet itself has experienced phenomenon growth in recent years hence, we state the following hypothesis:

Hypothesis 1. Most computer crimes and security breaches will exhibit size-based network externality phenomena.

We next discuss the various types of externalities and their influences on network attacks.

Exponential externality

Let us assume that \( g(\text{Int}_t) \) follows an exponential distribution (in short \( \text{exp} \)) as observed in the attack growth data, i.e.:

\[
g(\text{Int}_t) = \exp(\lambda*(\text{Int}_t)) \tag{7}
\]

where \( \lambda \) is a constant indicating size-induced growth.

The functional form is as follows:

\[
\text{SAttack}(t) = (f*\exp(K*B_{t}))*\exp(\lambda*(\text{Int}_t)) \tag{8a}
\]

\[
\log(\text{SAttack}(t)) = \log f + K*B_{t} + (\lambda*\text{Int}_t) \tag{8b}
\]

where \( f = \text{Attack}_0*\exp(c/q), \text{Attack}_0 \) is the cumulative number of attack incidents at time \( t=0 \), \( c \) is the net rate of instigations and \( q \) is the rate of inhibition, \( B = \exp(-q) \).

When \( \lambda =0 \), the equation reduces to a pure S-curve: \( \text{SAttack}(t) = \text{Attack}(t) \) (which is the PHM model) and which represents the diffusion effects only. When \( \lambda >0 \), the growth would represent an exponential one, reflecting the effect of network externality phenomenon.

Linear Externality

Let us assume that \( g(\text{Int}_t) \) follows a linear distribution as observed in the attack growth data, i.e.:

\[
g(\text{Int}_t) = (A+\lambda*(\text{Int}_t)) \tag{9a}
\]

\[
\text{SAttack}(t) = (f*\exp(\lambda* B_{t}))*((A+\lambda* \text{Int}_{t}) \tag{9b}
\]

where \( \lambda \) and \( A \) are constants and not simultaneously zero.

Logarithmic externality

The formulation of the logarithmic size-adjusted PHM model can also be done in a similar fashion.

\[
g(\text{Int}_t) = \log(e+\lambda*(\text{Int}_t)) \tag{10a}
\]

and

\[
\text{SAttack}(t) = (f*\exp(K*B_{t}))*\log(e+\lambda*\text{Int}_t) \tag{10b}
\]

where “\( e \)” is the natural logarithmic constant, approximately 2.71828.

We now formally state hypothesis 2. Let the null hypothesis be that the attack incident growth follows an S-curve. Let the alternative hypothesis be that attack incident growth follows an S-curve adjusted for network externality. The hypothesis whether size-based network externality phenomenon is significant for attack incident growths is tested for growth models.

Hypothesis 2. Network size-adjusted diffusion models will be better than the pure diffusion models as far as time-varying modeling of attack incidents is concerned.

DATA AND RESULTS

Data on attack incidents are sparse. Combining data from various sources also reduces the number of data points (10 years, in the present case). It may be mentioned that a few data points have been used in literature to model the diffusion process of an innovation, especially at an earlier stage of its growth (Mahajan and Peterson 1987). We next describe briefly the different data sets used in this paper.

Attack incident data

An attack is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An incident, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of attackers, and the degree of similarity of sites, techniques, and timing. The CERT/CC data records used in the present study were of incidents composed of numerous attacks (Howard 1997). The data set consisting of cumulative yearly data spans a period of 14 years from 1988 to 2001. Howard (1997) mentions several problems with the data, although researchers have used the data in many situations (Householder, Houle and Daughtery 2002). For a detailed description of the data and its use, the reader is referred to (CERT/CC 2001).
Attack type data

Attack type data (for testing hypothesis 1) were collected from the survey called “Annual CSI/FBI Computer Crime and Security Survey” sent to survey information security practitioners in U.S. organizations (Power 2002). The survey has been run with almost the same set of questions from 1987 to present. The data set from the survey of 2003 is used for the present study. The response rate for the 2003 survey was less than 20% with 530 practitioners responding. Richardson (2003) mentions that the statistical rigor of the CSI/FBI survey findings is sound.

The total annual loss data which is in U.S. dollar value is used. The annual financial loss data figures that reflect the most accurate situation is used in terms of the extent of financial damages incurred by firms by such attacks. The financial loss data figures were converted to 1996 U.S. dollar value by dividing by the price deflator for each year. The logarithmic value is used to keep the errors in check.

Network size data

In order to obtain network size data, the measurement of the Internet users per 1000 people in the U.S. was adopted from the World Bank (World Bank 2003). The U.S. data numbers were used, as 70% of all users and hosts of the world are from the U.S. and most attack incidents reported by CERT/CC are targeted toward the U.S. hosts and sites. Since we had data encompassing 10 years, our size-adjusted diffusion model contained 10 data points.

Results and Analysis

We first tested the hypothesis (hypothesis 1) that all computer crimes and security breaches exhibit size-based network externality phenomena. This hypothesis is supported in a limited way. As shown within Table 3, six out of nine types of attacks or misuses exhibit network externality phenomena as far as the size of the network is concerned. In other words, an increase in Internet network size shows an increase in attack activity in every two out of three types of attacks or misuse. This provides limited support for hypothesis 1.

Three attack types: unauthorized insider access, telecom fraud or active wiretapping did not show any relationship to network size. Active wiretapping and telecommunication fraud are not common, because these are inherently difficult to do, compared to other forms of attacks (Panko 2003). Active wiretapping is also highly under reported as even many governments secretly participate in this activity. Additionally, this type of attack growth is not directly dependent on the Internet growth.

Table 3. Correlation Results for Network Size Influence (1997-2000)

<table>
<thead>
<tr>
<th>FACTORS (Log of)</th>
<th>PEARSON CORRELATIONS</th>
<th>SIGNIFICANT (2-TAILED)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Users per 1,000 (size)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of Proprietary Information</td>
<td>0.9875</td>
<td>0.013*</td>
</tr>
<tr>
<td>Sabotage of Data of Networks</td>
<td>0.9678</td>
<td>0.032*</td>
</tr>
<tr>
<td>Telecom Eavesdropping</td>
<td>0.9960</td>
<td>0.004**</td>
</tr>
<tr>
<td>System of Penetration by Outsider</td>
<td>0.9951</td>
<td>0.005**</td>
</tr>
<tr>
<td>Insider Abuse of Net Access</td>
<td>0.9972</td>
<td>0.003**</td>
</tr>
<tr>
<td>Financial Fraud</td>
<td>0.9832</td>
<td>0.017*</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>0.9961</td>
<td>0.056*</td>
</tr>
<tr>
<td>Number of Virus</td>
<td>0.9890</td>
<td>0.011*</td>
</tr>
<tr>
<td>Unauthorized Insider Access</td>
<td>0.8547</td>
<td>0.145**</td>
</tr>
<tr>
<td>Telecom Fraud</td>
<td>0.8723</td>
<td>0.128**</td>
</tr>
<tr>
<td>Active Wiretapping</td>
<td>0.9267</td>
<td>0.245**</td>
</tr>
<tr>
<td>Laptop Theft</td>
<td>0.9804</td>
<td>0.02*</td>
</tr>
</tbody>
</table>

• * Correlation is significant at the 0.05 level (2-tailed)
• ** Correlation is significant at the 0.01 level (2-tailed)
• NS - not significant
Unauthorized access by insiders represents a broad section of such attacks. It is a fairly common and credible form of attack. IT staff members and security staffs of a firm often have very wide knowledge and access permissions (Panko 2003). Additionally, e-business has introduced the concept of global instant access to corporate data. Firms, in order to support this concept have opted for infrastructures that are based on open systems and networks. As a result universal access to a firm's infrastructure is extended to customers, partners, vendors, etc (Palisade 2003). The threat of attacks emanating from such accesses is real. A few examples will illustrate the point (Computer World 2001).

In 1997, a temporary computer technician at Forbes magazine was charged with crashing the company's network and causing more than $100,000 in damage. In 1998, a disgruntled programmer at Omega Engineering Corp. set off a digital bomb, destroying $10 million in data. Disgruntled employees and other insiders with legitimate access to critical business networks accounted for more than 80% of the cyber attacks against companies in 2000.

However, some of these attacks can be mounted on the internal network or an individual machine of the firm, thus making these independent of the Internet. Additionally, firms may not like to disclose this type of attack, for fear of losing customers and stockholders.

Telecom fraud can be wired or wireless in nature. According to Gordon and Loeb (2004), telecom fraud accounted for $3,997,500 and abuse of wireless network amounted to $10,159,250 in the year 2004. Accurate fraud figures are difficult to obtain and not all such frauds are related to the Internet infrastructure.

Many of these frauds are aimed at gaining financial advantages, committed by insiders and often are not reported. To quote an expert (Power 2002), "Most organizations do not make financial fraud incidents public because they do not want the bad PR, and they do not want federal law enforcement getting involved. It is often perceived as easier for the companies to take the loss. However, of the press releases that exist, most involve employees, former employees."

Hypothesis 1 provided preliminary evidence that size matters in Internet attack growth. We next focused on growth models. To observe the impact of the value of $\lambda$ (which measures the impact of size) on an exponential-sized PHM model, a few simulations were done for various $\lambda$ values. The growth curves are plotted against the pure diffusion curve of the PHM model. It is observed that as $\lambda$ is increasing in value (.004 to .01), the growth curves are rapidly increasing and the overall curve shows an exponential like pattern. This is shown in Figure 2.

To answer graphically whether the growth pattern is closer to the pure logistic model or the PHM model, a plot of $D\Delta$tck was done on $Attck$ (Figure 3(a)) and log ($Attck$) (Figure 3(b)). $D\Delta$tck is the growth rate of logarithm of $Attck$ or $D\Delta$tck = $d(\log(Attck))/dt$.

We take the discrete analog of $D\Delta$tck :

$$D\Delta$tck = \log(Attck_{t+1})/\log(Attck_t)$$

When $D\Delta$tck is plotted against $Attck$, $D\Delta$tck should resemble a decreasing linear function of $Attck_t$ (as in the case of the logistic model). However, the fit to a linear decreasing function is poor ($R^2$ of linear fit=0.14), as shown in Figure 3(a). As the PHM model formulation implies, $D\Delta$tck, when plotted against log($Attck$) should resemble a decreasing linear function of log($Attck$). Indeed it is much closer to a linear decreasing function ($R^2$of linear fit=0.76) as shown in Figure 3(b). This analysis shows the better model fit of the PHM model over the logistic model. One can expect that size-adjusted PHM model will also provide better fit than the corresponding size-adjusted logistic model.

Tables 4-6 include the summary of non-linear regression results containing estimates of different models, and Figure 4 shows the fits obtained from the two best models (the PHM model and extended PHM model with exponential network size). The non-linear least square technique was used to estimate the parameter values. Earlier results showed that the PHM model performs better than other traditional growth models (Bagchi, Solis, and
Figure 2. \( \lambda \) Values and Their Impact on the Overall Exponential Sized Growth-curves

Figure 3(a). The plot of D\text{Attck}_t against \text{Attck}_t.
The PHM model showed a reasonably good fit with $R^2$ value of 0.97.

Next, the PHM model was compared to its extensions based on network size. Results are shown in Table 4. The model extension with log (network size) was eliminated from consideration as simulations showed that the log’s fit was the worst of all models. Although the pure PHM model (model 1) provides a good fit, model 2 (PHM model extended with an exponential size) shows a better fit ($R^2$ value = 0.99), and the value of $\lambda$ in model 2 is statistically different from zero ($p<.000$). Therefore, the null hypothesis that $\lambda = 0$ can be rejected for model 2, and it can be concluded that exponential size assumption has a significant impact on the growth of attack incidents. Model 3 (Table 4), which is an extension of PHM model with a linear network size, is poor in estimates with the lowest $R^2$ value (0.96). The extended logistic model with exponential size (model 4) was also considered. The extended logistic model provides a good fit ($R^2$ value = 0.99) and again shows that the size-extended model is a better fit than the pure logistic model.

So from a model fit point of view, the best two models are: model 2 (the extended PHM model with exponential size) and model 4 (the extended logistic model with exponential size). However, since the extended logistic model’s explainability is poorer than the extended PHM model with exponential size, we select extended exponential size-adjusted PHM model (model 2) as the best model for the attack incidents. The fit of extended PHM model (model 2) was also better than the extended logistic model (model 4). When measured in terms of sum of absolute deviations of the estimates from the actual data, the sum of absolute deviations was larger for the extended logistic when compared to the extended PHM model (29,553.13 against 17,557.7). Figure 6 shows the estimates from the PHM model and an extension of the PHM model with exponential size. Table 5 shows a few sample data values and estimates.

The general pattern of the rate of attack growth appears to be explained better by the size-incorporated security model. This supports hypothesis 2. The best model (model 2, extended size-adjusted PHM), however, still underestimates the actual growth somewhat. In order to empirically test the superiority of the size-adjusted model over the pure PHM model, we employed Davidson and Mackinnon’s P-
Table 4. Parameter Estimates and Model Fits from a Few Selected Models

<table>
<thead>
<tr>
<th>Model 1. Pure Attack Incident Model (PHM model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c=9; \quad q=.04$</td>
</tr>
<tr>
<td>Overall $R^2 \quad 97$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model 2. Network size-adjusted PHM model: $\log[S\text{Attck}(t)]=\log f + K \cdot B^t + \lambda \cdot \text{Int}_t$ (network size is exponential)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>$\log f$</td>
</tr>
<tr>
<td>$B$</td>
</tr>
<tr>
<td>$K$</td>
</tr>
<tr>
<td>$\lambda$</td>
</tr>
<tr>
<td>$c=1.287, \quad q=0.274$</td>
</tr>
<tr>
<td>Overall $R^2 \quad .99$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model 3. Network size-adjusted PHM model: $S\text{Attck}(t)=(f^* \exp(K \cdot B^t ))*(A+\lambda \cdot \text{Int}_t)$ (network size is linear)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>$A$</td>
</tr>
<tr>
<td>$\log f$</td>
</tr>
<tr>
<td>$B$</td>
</tr>
<tr>
<td>$K$</td>
</tr>
<tr>
<td>$\lambda$</td>
</tr>
<tr>
<td>$c=.01, \quad q=.10$</td>
</tr>
<tr>
<td>Overall $R^2 \quad .96$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model 4. Network size-adjusted Logistic Model: $[1/S\text{Attck}(t)]=(K+C \cdot B^t ) \exp(-\lambda \cdot \text{Int}_t)$ (network size is exponential)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>$C$</td>
</tr>
<tr>
<td>$B$</td>
</tr>
<tr>
<td>$K$</td>
</tr>
<tr>
<td>$\lambda$</td>
</tr>
<tr>
<td>Overall $R^2 \quad 99$</td>
</tr>
</tbody>
</table>

Table 5. Some Examples of Actual data and Estimates

<table>
<thead>
<tr>
<th>Cumulative Attack Incident data</th>
<th>Year</th>
<th>PHM with Exp. Network-size-included (Model 2)</th>
<th>Pure PHM model (Model 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>390</td>
<td>1990</td>
<td>362.67</td>
<td>237.6</td>
</tr>
<tr>
<td>2903</td>
<td>1993</td>
<td>2870.37</td>
<td>3262.8</td>
</tr>
<tr>
<td>7655</td>
<td>1995</td>
<td>6921.25</td>
<td>9376.1</td>
</tr>
<tr>
<td>12362</td>
<td>1997</td>
<td>13569.65</td>
<td>19026.56</td>
</tr>
<tr>
<td>25955</td>
<td>1999</td>
<td>27318.74</td>
<td>30577.22</td>
</tr>
<tr>
<td>47711</td>
<td>2000</td>
<td>39261.98</td>
<td>36420.26</td>
</tr>
</tbody>
</table>
Figure 4. Estimates from Two Attack Incident Models

Two P-tests were done using the PHM model and the size-adjusted PHM model respectively as null models. The results of the test are shown in Table 6. We found that the size-adjusted PHM model is the true model as the test shows that the size-adjusted PHM model could eliminate the PHM model (insignificant p-value of .148>.001); however, the converse is false. The reverse test showed that the size-adjusted PHM model could not be eliminated by the PHM model (significant p-value of .000<.001). The tests showed the superiority of the size-adjusted PHM model over the pure PHM model, thus partly supporting hypothesis 2.

**SUMMARY**

An initial correlation analysis of twelve attack types showed that an increase in Internet network size is related to an increase in attack activity in every two out of three types of attacks or misuse. Next, several size-adjusted

<table>
<thead>
<tr>
<th>Null Model</th>
<th>Alternative Model</th>
<th>PHM</th>
<th>Size-adj. PHM</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHM</td>
<td>N/A</td>
<td>-1.66NS</td>
<td></td>
</tr>
<tr>
<td>Size-adj. PHM</td>
<td>8.14***</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

***p<.001; NS-not significant; N/A-not applicable
growth models were introduced to analyze the Internet attack phenomenon over time. From a previous study we observed that an attack incident model (PHM model) outperformed other traditional models used in a growth study (logistic, exponential, etc.) (Bagchi, Solis and Udo 2003). As mentioned earlier, the PHM model has two components, the net rate of instigation, c (0.90), and a rate of inhibition, q (0.04), in which a combination can reflect the true process of attacks. The imitation part of the model captures the rate at which people are influenced by other attacks; the inhibition part of the model captures the deterrence strategies implemented. Deterrence activities inhibit others from engaging in security attacks. The results show that the net imitation coefficient is much stronger than the inhibition coefficient for the data set. Imitation effects are stronger as attack incidents often get strong publicity. Thus Model 1 (PHM model) provided better fit and explainability than traditional growth models (logistic and exponential).

Next the PHM model was compared to several extensions of the PHM model as well as an extension of the logistic model with network size incorporated (Table 4). In these models (models 2-4), the diffusion theory based growth explained the growth process in the earlier part. The later part of growth was explained better by the network externality theory—network size plays an important role in the growth of attack incidents. Model 2, which is an extended version of the PHM model augmented with an exponential size, improved upon the original PHM model in both model fit and explainability of the attack incidents by including the exponential network size effect. The model also performed marginally better than the extended logistic model with size. The impact of \( \lambda \) (size effect) as calculated from this model is 0.4% of growth per year. The values of two other components of the model, the net rate of instigation, c, and a rate of inhibition, q, were 0.1 and 0.01 respectively. The value of size coefficient (\( \lambda \)) was 0.081 or 8.1 % of the growth per year. Model 4 is an extended logistic model augmented with an exponential size. It also provided a better fit than the pure logistic model, showing again that network externality matters. The value of the size coefficient (\( \lambda \)) was 0.028 or 2.8 % of the growth per year. The fit from the model (model 4) can be compared to model 2, although as discussed above model 2 provides a better fit; however, model 2 clearly is richer in providing a better explainability of the attack phenomena: it gives us estimates of net instigation rate, inhibition rate, and impact of the network size.

**CONCLUSIONS**

The implication of the findings of this preliminary study is that the number of incident attacks can be better predicted by considering an exponential network size effect. This finding has implications for practitioners. Since the number of network attacks is expected to grow as the size grows, firms need to implement the latest security software to protect their systems. Note also that unless better investments in designing error-free software and applications and in security technologies are made and unless more firms embrace security technologies, the attack incidents may grow in this fashion as the network size continues to grow exponentially and deterrence effects are minimal compared to the overall attack effects (as results from model 2 and others show). In the CSI/FBI survey of 2002, for example, only 90% of respondents said that they were using anti-virus software (CSI/FBI 2002). It was also noted that viruses were the type of attack that most frequently resulted in financial loss. Pipkin, Rubin, and Schindler (2002) think that most firms do not spend enough money to protect themselves, and many IT administrators have little control of their own networks.

The Internet growth is still strong and shows no signs of abatement. This study captures the attack incident growth process in its early stages and so is based on a limited data set of 10 years (limited due to availability of attack incident and size of the network data). Two points are worth noting. First, the attacks
are still in an earlier stage of development and many innovations (including bad ones) exhibit exponential growth at an earlier stage (Rogers 2003). Our present results show that. Second, the attack growth depends on, among other things, security measures taken that are at best inadequate at the present time as our results show (the inhibition coefficient value is much lower). Empirical evidences show that defensive mechanisms are mostly reactive in nature. If proper security mechanisms are in place, the situation might improve and influence of network size factor may prove to be less important in the future.

As the Internet grows, perhaps the growth process will start behaving more like an S-curve, as a sustained realization of exponential growth for a long time is difficult. Metcalfe also observes this in his seminal article (Metcalfe 1995). It is possible that the attack incident growth will also exhibit a similar S-curve pattern.

In this paper we considered network size as a major factor that influences attack incidents. We have earlier detailed many possible factors that are responsible for such attacks and in future can be investigated in detail as a research project. Most of these are expected to be related positively to the size of the network: the larger the size of the Internet, the greater is the volume of such attacks. There could be other additional factors that may affect network attack incidents. One other possible factor is the young Internet user population size that probably is strongly correlated to the size of the Internet considered in this paper. According to experts, attackers have been traditionally young, although the demographics are changing in recent times (Pipkin, Rubin, and Schindler 2002). The modern day young attackers do not even need thorough knowledge on creating an attack. Some of them, called script kiddies, possess only modest skills but use freely available attack scripts created by experienced hackers. These easily-available scripts make it easy to mount random attacks against firms by millions of script kiddies. Since these people are young and are under legal age, firms find it difficult to press serious legal charges and/or face unwanted publicity (Panko 2003). The same absence of legal sanctions prevents firms to pursue virus writers and releasers. Virus writing is not a crime in many nations and tracking a virus releaser is not easy. Attack automation is another trend that increases the volume of attacks. Mass automation robots can do billions of dollars of damage in a few hours.

Several other possible factors in the increase of network attacks are: infrastructure facility to access the Internet and a drop in Internet access prices. All of these possible factors may have a strong correlation to the size (as a drop in price increases the accessibility and therefore the Internet use increase). Future research should investigate these various factors and their conjectured empirical relationships with the size of the Internet. As an example, consider the effect of income of the population of a nation. Considering the period from 1991 to 2001, for example, we found that the number of attack incidents was strongly correlated to the U.S. GDP at the purchasing power parity (PPP) (Pearson’s correlation coefficient=0.80, p<.003). However, since the number of Internet users is also strongly correlated to the U.S. GDP PPP for the same period (1991-2000) (Pearson’s correlation coefficient=0.94, p<.000), the effect of GDP can be partly taken care of by the size of the network.

Considering the deterrent side of such attacks, many technological solutions exist that can reduce the number of such attacks (Panko 2003). Proper access control, training and enforcement, encryption of messages, use of anti-virus software, downloading and implementing the latest software patches for the software used, use of penetration defensive tools such as firewalls, IDS etc., can be applied to reduce such attacks. Security auditing is required to ensure that planned protections are working. However, it is prudent to note that security is a management issue and not a technological one. At any firm, a total commitment to security management is required. Finally, cyber war and cyber terror are threats that can cause unmitigated damages in future. National security planning is required to counter such attacks.

There are several shortcomings of the work. These are related to the nature of the data. First, the security attack incidents reported may not be exhaustive. For example, the FBI reports that only 17% of actual attack incidents are reported (Sofaer and Goodman 2000). A more accurate nature of data should
include a higher percentage. Second, the time stamps of the incidents in the earlier phases of reporting in CERT/CC may not be exact (Howard 1997). However, these have not deterred researchers from using the same data source for other studies (CERT/CC 2001), (Householder, Houle and Daughtery 2002), (Moitra and Konda 2004), (Shimeall and Williams 2003).

Implications and future research

The above findings may be useful to firms. One implication of the study is that the current increase in attack incidents is not a fad but rather may have a theoretical basis. Our findings suggest that an increase in Internet network size is related to an increase in attack or misuse incidences, which implies that organizations with large networks should pay even greater attention to their network safety. Government and firms should recognize that the present spending in attack-preventing measures should be increased to prevent more attacks of this kind.

In order to make a detailed and thorough future investigation on this aspect we need reliable time series data of various types of attacks for an extended period of years.

In future, we plan to extend and test some of these models on various security attack types. We also plan to do a Delphi on what can inhibit the trend in attacks in future. Some of the interesting issues for future research, subject to data availability, are: what factors are responsible for such network attacks, detecting possible smaller waves of contagion within the large wave of attacks, detecting any exhaustion effect resulting from negative impact of such attacks, if any (Myers 1997). Forecasting is an essential component of any model design (Franses 1998). We have designed a new model and presented the model in this paper. However, for reliable forecasting purposes, we need several years of additional data. A future work can deal with the issue of forecasting based on the size-adjusted model. Finally, as more data become available, one can reexamine the growth pattern to see if exponential size-adjusted growth has changed.

Acknowledgement. The authors wish to thank the anonymous reviewers for their helpful comments which improved the quality of the manuscript.

REFERENCES


Kallol Bagchi and Zaiyong Tang


AUTHORS

**Dr. Kallol Bagchi** is an assistant professor of Information and Decision Sciences at the University of Texas at El Paso. He received his Ph.D. in information systems from the Florida Atlantic University. Prior to pursuing his IS doctorate, he had earned a Ph.D. degree in Computer Science from India. He has worked in both industry and academia and has published in journals such as *International Journal in Electronic Commerce, Communications of the AIS, Electronic Journal of Information Systems in Developing Countries* and *Journal of Global Information Technology Management*. He has also presented papers in a number of national and international conferences. His current research interests include IT adoption and diffusion, Internet security, Global IT, Electronic commerce.

**Dr. Zaiyong Tang** is an assistant professor in the Department of Management and Information Systems at Louisiana Tech University, USA. He obtained his Ph.D. in MIS from the University of Florida; an M.S. from Washington State University; an M.E. from Chengdu University of Science and Technology; B.E. from Chongqing University, P.R. China. His research interests include information technology diffusion, artificial intelligence (in particular, intelligent agents), neural networks, knowledge management, and agent-based modeling. His work has appeared in *INFORMS Journal on Computing, Information and Management, Simulation*, and *Neural Networks*, and various conference proceedings.