A Human-Centric Approach to Simulation of IS Security Dynamics

Mark Rounds, University of Idaho, Moscow, ID 83844, USA; E-mail: mrounds@uidaho.edu
Norman Pendegraft, University of Idaho, Moscow, ID 83844, USA
Carol Taylor, University of Idaho, Moscow, ID 83844, USA

ABSTRACT

This paper outlines a new approach to computer security using simulation to study computer security policy. We suggest that understanding the interactions between humans and information systems is central to creating effective security policy. Most previous research has focused on technical issues of system vulnerability or computer security tools. Our approach employs simulation models in order to understand how attackers and users react to varying levels of parameters such as computer security and system value.

1. INTRODUCTION

Computer security is a human-centric problem with humans actively involved in both the attack and defense of systems. Consequently, we believe that a new approach is needed that places human activity at the center of a model that shows trade-offs between human choices as security is varied.

In this paper, we develop a simple economic model to examine interactions between users and attackers. Despite its simplicity, the model is too complex to provide clear policy recommendations. Hence we advocate simulation as a means of further study of these systems. We develop a framework for that simulation which should allow managers to experiment with policies before implementation. This paper does not provide simulation results as we do that elsewhere (Pendegraft and Rounds 2006, Pendegraft, Rounds, and Frincke 2005) and is intended as an apologia for the approach.

Subsequent sections of the paper cover some background (Section 2), our modeling approach and background on users and attackers (Section 3), and research agenda (Section 4).

2. BACKGROUND

The security literature has grown significantly in the last decade. However, the focus of most researchers has been on technology: intrusion detection, encryption, system management, etc. There has been relatively little discussion of the behavior of the humans involved or of the interactions between them. Even Saltzer and Schroeder (1975), who recognize that humans play a role, focused on the technological issues of security rather than the interactions of the system with its users and attackers.

Security imposes a cost on the user. According to Sasse et.al (2001) and Sasse (2003), complex multiple passwords are beyond the capability of human memory. This increase the need for user support which imposes further costs. Fixes to this problem, i.e. writing down passwords or automated password retrieval have security and cost issues of their own. These issues have not received enough attention from the security community. Recognizing the cost of security, many firms engage in cost benefit analysis of security measures before imposing them (Gordon et.al. 2006),

There is a considerable literature examining the impact of system quality on user behavior which supports our belief that system value increases use. The Technology Acceptance Model (Davis 1989) offers a means of analyzing the impact of ease of use upon usage. The IS Success model (ISM) explicated by DeLone and McLean (1992) includes constructs of information and system quality and posits that system and information quality lead to increased user satisfaction and increased use which in turn leads to net benefits. DeLone and McLean (2003) recently revised that model to expand measure of quality to include service quality and to explicitly include a feedback loop from net benefits to intention to use. Wixom and Todd (2005) recently integrated the two models and their results suggest that there is a link between system and data quality and the one hand and system usage on the other. Zhu and Kraemer (2005) argue that firm value is increased by IS usage in E-business applications.

3. MODELING APPROACH

3.1. Preliminaries

Our research uses an economic point of view rather than that typical of the computer security literature. In the economic analysis if crime typified by Becker's landmark work (1968) a system of equations is developed which describes in some aggregate way the behavior of criminals. Block and Heineke (1975) extend that work to consider the labor cost incurred by the criminal.

This approach focuses attention on societal value using a utility function about which only limited assumptions are made. In our context this translates to looking at system value rather than maximizing security or minimizing attacks. It also translates into response functions which are inherently inexact. Such ambiguity is seems inherent in the approach. For example Block and Heineke (1975, p315) use one term to represent the "failure, capture, or arrest rate" with criminal behavior. While the ambiguity is unfortunate, it does focus attention on aspects of the problem that are not well understood and therefore suggests fruitful avenues for future research.

In the next section we develop a simple two player model patterned on Becker's economic analysis of crime. As will be seen the model becomes very complex and is inherently static. In response, we will argue for simulation as a preferred mode of inquiry. Simulation offers the addition advantage of allowing us to investigate non linear behavior. Given the apparent interaction between users and attackers, it seems likely that computer security will have non linear interactions.

3.2. Economic Model

We assume that users and attackers both are motivated by the current value of the system and by the current level of security. We also view the problem of IS security as essentially dynamic, that is, we assume that the behavior of the system over time is of interest; hence we use time as an independent variable.

We adopt the following notation.

U : level of use by user	=U(V,S)
A : level of attacks	=A(V,S)
V : current value of the system	=V(T)
S : current level of security	=S(T)
T : time	

We assume that these functions are sufficiently well behaved that we may determine their derivatives. We will use the following notation: X' = dX/dT and X_y will be the partial derivative of X with respect to Y.

We calculate the time rate of change of each player's action:

$$\frac{dU}{dT} = \frac{\partial U}{\partial V}\frac{dV}{dT} + \frac{\partial U}{\partial S}\frac{dS}{dT}$$

$$\frac{dA}{dT} = \frac{\partial A}{\partial V}\frac{dV}{dT} + \frac{\partial A}{\partial S}\frac{dS}{dT}$$

At equilibrium these must both be 0 so we have

$$\frac{\partial U}{\partial V}\frac{dV}{dT} + \frac{\partial U}{\partial S}\frac{dS}{dT} = \frac{\partial A}{\partial V}\frac{dV}{dT} + \frac{\partial A}{\partial S}\frac{dS}{dT}$$

$\frac{V'}{S'} = \frac{A_S - U_S}{U_V - A_V}$. Hence,

$$\frac{dV}{dS} = \frac{A_S - U_S}{U_V - A_V}$$

Now this means that dV/dS > 0 in two cases.

1. $U_v > A_s$ and $U_s < A_s$
2. $U_v < A_s$ and $U_s > A_s$

Since $U_v > 0$, $A_v > 0$, $U_s < 0$, and $A_s < 0$, this gives

$U_s < A_s < 0 < A_v < U_v$
$A_s < U_s < 0 < U_v < A_v$

We take the second to be the more common situation. In that case, attackers are more sensitive both to the value of the system and to the security level. There is a possible policy implication here, in that if neither of these conditions obtains, addition security may be counter productive.

Now we extend to consider a dynamic model. First consider the case where the security policy is static, i.e.

$$\frac{dS}{dT} = 0$$

Then

$$\frac{dA}{dT} = \frac{\partial A}{\partial V}\frac{dV}{dT}$$

Since we have assumed the first term positive, this means A' has the sign of V_t. If we allow dynamic security, then $A' = A_v V' + A_s S'$. Since $A_s < 0$, $S' > 0$ will cause a reduction in A' (Note that it does not directly affect A, rather the time rate of change of A.) This suggests the following policy:

If A'>0 then increase S (ie make S'>0)

If A'<0 then decrease S (ie make S'<0) This follows since it will apprarenlty result also in increased usage which is assumed to be a good thing.

Now, it seems reasonable to assume that V'=V'(A,U,V). In particular, we assume that

$\frac{\partial V'}{\partial A} < 0, \frac{\partial V'}{\partial U} > 0, \frac{\partial V'}{\partial V}$ indeterminate in sign.

The attacker's problem is now

$$\frac{Max}{A}\alpha(V, S, A)$$

And the user's problem is

$$\frac{Max}{U}\beta(V, S, U)$$

Block and Heineke's analysis follows these lines for only the attacker, and leads to results of limited utility for our scenario. Their results apply at equilibrium which seems inappropriate for us and excluding the impact of usage on a system is clearly not realistic in our case because it is precisely the use of these systems that makes them valuable. Note also that we are not concerned with the direct interaction between user and attacker. Rather the attacker affects the user only indirectly by reducing the value of the system, thus reducing the user's level of use.

The net result is that is seems unlikely that the sort of analysis demonstrated here will lead to generally useful insights. It is well know that solving complex systems of differential equations is hard, and the standard way to study dynamic systems is via simulation.

3.3. General Simulation Model

Our approach to simulation is consistent with Senge (1990) which in turn drew from Forrester's work at MIT on systems dynamics (1961). Like the forgoing analysis, this approach takes a top down point of view.

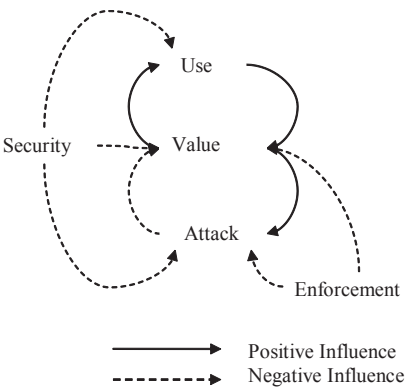
Systems dynamics models use two types of objects: reservoirs and flows. Reservoirs represent constructs whose values change over time, and the flows represent changes in the values of those constructs. In effect, the flows are derivatives of the reservoirs. Our modeling tool IThink, (High Performance Systems) converts these models into a set of finite difference equations which are solved numerically. Our models are simple because as Senge and IThink point out, simple models are much easier to understand. There is also the problem of exploding state space as models become more complex.

The basic model is illustrated in Figure 1. The main constructs are value, use, and attacks. Solid lines indicate a positive or increasing influence; dashed lines indicate a negative influence. The model shows that increases in value cause increases in use and attacks. Use increases value while attacks decrease value. Security reduces both use and attacks and has a cost (i.e. reduces value). Enforcement acts only against attacks, also at a cost.

3.4. Value and Security

System value is the key parameter in our model. Previous work (Sasse 2001, 2003, Pendegraft and Rounds 2006) has shown that value is a complex parameter. A user may assign a value based on the amount of data the system holds and the ease with

Figure 1. Value model



which it can be extracted. For a customer, the ability to carry out a transaction quickly, accurately, and securely may also enter into their view of value.

Some attackers are motivated by money (Richmond 2004). An attacker may view value as the number of records that can be extracted for sale. An attacker with a political agenda may care more about the identity of the system owner than the intrinsic value of the data. Clearly a major item in our agenda will be to clarify the aspects of system value that drive human behavior. In some sense, this extends the work of Jonsson and Olovsson, (1997) and relies upon the definition of information system value (Walters and Lancaster 1999).

Similarly, our notion of security is simple. We model security as a single parameter ranging from 0 to 1 reflecting a completely open system to one which is inaccessible. Like value, security is multifaceted and clarifying what security is must be an essential item in our agenda.

3.5. Impact of Security and Value on Behavior

We model the impact of security and value on attackers and users as S shaped. While there is some support for this idea in the error detection literature (Yamada, Ouba, and Osaki, 1983) it remains to confirm the idea experimentally. Figures 2 and 3 illustrate this postulated behavior. Figure 2 illustrates the idea that use and attacks increase with increasing rate at low levels of value, and then with decreasing rate. Figure 3 shows use and attacks decreasing slowly with increasing security at low levels of security, and then decreasing rapidly, and finally decreasing at a reduced rate. Note that we do not assert (nor believe) that these curves are identical for users and attackers, rather that they have the same general shape.

For the purposes of this research we model attackers as rational criminals with a common response curve. While there are many sorts of attackers this simplification makes the results much more understandable. We base the rational activities of our attacker upon the economics of criminal activity (Becker 1968). Finally, it is clear that attacks on a system reduce its value. While firm value is only part of our notion of value, there is evidence that firm value can be reduced by cyber attacks (Garg, Curtis, and Halpner 2003; Miora and Cobb 1998; Saita 2001, Olavsrud, 2001).

3.6. Enforcement and Security

We understand security to be actions which reduce the likelihood of success and severity of attacks. We also understand that security imposes costs on users. Enforcement includes active steps taken to reduce the number of attackers. It includes law enforcement and actions taken by targeted companies.

Traditional law enforcement has not been especially successful in dealing with cyber crime, (Jayaswal, Yurcik, and Doss, 2002) and may impose additional costs on the victims. Department of Justice's (2002) guidelines call for seizure of the victim's hardware under certain circumstances hardware seized from the victim is reclaimed only with much difficulty (Holtzman 2003).

There are reports that some firms have engaged in direct efforts to retaliate against hackers and reduce their numbers. (Schwartau 2000, Radcliff 2000, Thayer 2005).

Figure 2. Value

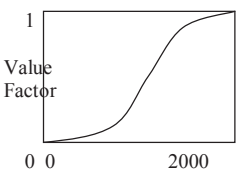
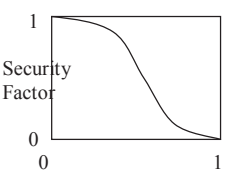


Figure 3. Security



There are a number of products available to facilitate counterattacks (Farber 2002, Secure Computing 2005).

4. CONCLUSION AND FUTURE WORK

Despite increasing expenditure on computer security computer crime continues to be a problem. The traditional computer security literature focuses on technical issues. We have developed a complementary point of view which emphasizes system value and the interactions between the system and its users and attackers. We continue to examine these questions via simulation.

We have made a number of simplifying assumptions. Clearly these are open to challenge. To validate and expand our models some of these assumptions will require experimental examination of some issues like the response of attackers and users to changes in system value and security. Our goal, as described in our introduction, is to focus on interactions in hopes of gaining new and interesting insights into the security problem. We hope that other researchers will find these questions interesting and join us in our efforts to investigate them.

5. REFERENCES

Becker, Gary S. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy 78, 169-217.

Bindview. (2005). http://www.bindview.com/Services/RAZOR/Utilities/Unix_Linux/ZombieZapper_form.cfm

Block, M.K. and Heineke, J.M.. (1975). Labor Theoretic Analysis of Criminal Choice. American Economic Review 65, 314-325.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MISQuart 13(3), 319-340.

DeLone, W.H. and McLean, E.R. (1992). Information System Success: The Quest for the dependent Variable. ISR 3(1) 60-95.

DeLone, W.H. and E.R. McLean, E.R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. JMIS 19(4) 9-30.

Department of Justice. (2002). "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf.

Farber, D. (2002). "Miracle cure for security woes?". ZDNet August 5th, 2002, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2876552,00.html.

Forrester, Jay W. (1961). Industrial Dynamics, MIT Press.

Garg, A., Curtis, J., and Halper, H. (2003). "The Financial Impact of IT Security Breaches: What Do Investors Think?". Information Systems Security, March/April.

Gordon, G.,A., and Loeb, M. P. (2002). The Economics of Information Security Investment. Transactions on Information and System Security (TISSEC). Volume 5 , Issue 4 November 438-457.

Gordon, G., Loeb, M., Lucyshyn, W., and Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

High Performance Systems, IThink / Stella Technical Documentation, Lebanon NH.

Holtzman D. (2003). "If You Can't Stand the Heat, Don't Call 'Em" CSO Magazine. July 2003.

Information Security Oversight Office (ISOO) (2004) Information Security Oversight Annual Report, http://www.archives.gov/isoo/reports/2004-cost-report.html

Jayaswal V., Yurcik, W., and Doss, D. (2002). "Internet Hack Back: Counter-Attacks as Self-Defense or Vigilantism." Proceedings of the IEEE International Symposium on Technology and Society, Raleigh, USA, June

Jonsson, E. and Olovsson, T. (1997). "A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior," IEEE Trans. Software Eng., Apr. 1997, pp. 235-245.

Olavsrud T. (2001). "Egghead Files for Bankruptcy, Plans to Sell Assets", Internet News August 15th 2001 www.internetnews.com/ec-news/article.php/866871.

Pendegraft, N., Rounds, M. (2006). "A Simulation of IS Security with Variable Attacker Populations", working paper.

Pendegraft, N., Rounds, M., and Frincke, D. (2005). "A Simulation Model Of IS Security". 43rd ACM Southeast Conference, March 18-20, 2005, Kennesaw, GA

Radcliff, D. (2000). "Should You Strike Back?". Computer World Nov 13,

Richmond, R. (2004). Money Increasingly Is Motive For Computer-Virus Attacks. Wall Street Journal, 19 Sept., B5.

Saita, A. (2001). "On the Cutting Edge" Information Security, February 2001 http://infosecuritymag.techtarget.com/articles.february01/departments_news.shtml.

Saltzer J., and Schroeder, M. (1975). "The Protection of Information in Computer Systems, Proc. IEEE, vol. 63, no. 9, 1975, pp. 1278-1308.

Sasse, A., (2003). "Computer Security: Anatomy of a usability disaster, and a plan for recovery", Proceedings of CHI 2003 Workshop on HCI and Security Systems, Fort Lauderdale, Florida.

Sasse, A., Brostoff, S., and Weirich, D. (2001). "Transforming The Weakest Link – A Human Computer Interaction Approach To Usable Effective Security". BT Technological Journal, No 19, pp 122-131.

Schwartau W. (2000). Can You Counter-Attack Hackers?. NetworkWorld. April

Secure Computing, (2005). http://www.securecomputing. com/index.cfm?skey=1303

Senge, P.M. (1990). The Fifth Discipline, Currency Doubleday, New York.

Thayer, R. (2005). "Hack … hack back … repeat". Network World. August 9th, 2004, http://www.networkworld.com/news/2004/080904defcon.html.

Walters D., and Lancaster, G. (1999) "Value And Information: Concepts And Issues For Management". Management Decision. Volume 37 Issue 8, pp 643.

Wixom, Barbara and Todd, Peter, A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. ISR16(1) 85-102.

Yamada, S., Ouba, M., and Osaki, S. (1983). "S-Shaped Reliability Growth Modeling for Software Error Detection," IEEE Transactions on Reliability, R-32, 5, December 475-478.

Zhu, K. and Kraemer, K. L. (2005). Post-Adoption Variation in Usage and Value of E Business by Organizations: Cross-Country Evidence from the Retail Industry. ISR 16(1) 61-84.