PRELIMINARY SIMULATION OF HACKER TARGETING DECISION

Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow, ID 83844-3161
Mark Rounds, College of Business and Economics, University of Idaho, Moscow, ID 83844-3161

ABSTRACT

A model of two hosts with a single attacker and single defender each allocating resources to attack / defend two information systems is presented. The model shows that simple strategies like diversification may have merit, but that more complex strategies are hard to develop.

INTRODUCTION

In previous work [7] presented system dynamics models of information systems under attack. Here we extend that work to allow for two hosts. The attacker and defender are presumed to allocate their efforts, perhaps dynamically, in attack and defense of the hosts. Dutta and Roy [3] conducted a simulation based on systems dynamics that looked at the security problem at an organizational investment level. Martinez-Moyano et.al. [6] developed a dynamic systems model focusing on the number of security measures to be implemented. Their results emphasize the possibility that excess security measures may in the long run reduce the security of a system.

In some sense this work follows in the line of similar work dealing with economics [10], crime [1], terrorism [9], and warfare [12]. While the assumptions that we make about the objects are different from those in the other literatures, the overall structure of the model is similar.

This approach is inspired by Senge [11] who in turn drew from Forrester's work on systems dynamics modeling [4]. Our model uses "value" as a system metric. In other words, we assume that managers desire to maximize system value rather than maximizing security or minimizing attacks. Some ambiguity is inherent in this approach. Similar ambiguity is found in the economics of crime literature. For example, Block and Heineke [2] use one term to represent the "failure, capture, or arrest rate" with criminal behavior. As we note below, one of the major problems is IS security management is uncertainty over what to monitor, so this suggests fruitful avenues for future research.

The model detailed in this paper increases the number of information systems to two. This seems like a small change to the model, however this effectively doubles the state space which was already too large in Pendegraft and Rounds [7] and warned against by Holstein [5]. The attacker must now also decide on which information system to attack based on perceived value and hardness. The defender has to decide how to allocate limited resources to defend both information systems and whether or not to respond dynamically.

One of the major issues in IS security research is that we don't know what parameters of systems need to be measured. One of the major long term objectives of this line of research is to shed light on this issue by building various assumptions into our models and seeing which ones have traction.

Our primary interest in this paper is to validate the model to ensure that it reacts reasonably to typical circumstances. In this respect the model is a success. It has also focused our attention and several issues which are commonly ignored in the IS security literature: namely motivations of users and attackers. In

particular, we found that modeling the decision rule for attackers is hard and has been largely ignored in this literature. This is in our opinion a serious shortcoming, one that we are addressed experimentally in other work.

There are a number of limitations to this sort of research. Two are of particular note. First, the models capture general behavior only. This stems from the fact that no effort is made to determine exact macro-economic values for the various parameters. Instead, only the relative shapes of the responses are determined. The second is that the size of the state space precludes evaluation of all cases. Since the model used is a significant extension of our previous models, our primary objective is to validate its general structure and do some preliminary investigation of its behavior and implications. IThink recommends adding no more than a few objects object between model extension [8]. We have here, of necessity, approximately doubled the size of our previous model.

MODEL

The simulation was built in IThink. The static model is shown in figure 1. This model was subsequently extended to allow for dynamic polices on the part of both the attackers and users. In developing the model, we adhered to a number of assumption. In particular, we assumed that:

-value increases with use and decreases with attacks.
-there will be some use regardless of value.
-use and attacks increase with value and decrease with attacks.
-attackers use a simple policy to allocate attacks (proportional to V).
-attackers and users have S shaped responses to value and inverted S shaped responses to security.

The second assumption merits discussion. Value is the perception of the players. As we were discussing this issue in preparing the paper, one of us was distracted by email, and commented something like, "I hate email'. The other observed that this event showed that we are frequently obligated to use systems that we perhaps do not value. Hence we kept the assumption. In the current model, these are implemented with piece wise quadratic forms. To simplify our management of the model, parameters were chosen so that in the static, symmetric case values of the systems doubled in about 100 iterations.

RESULTS AND DISCUSSION

We ran the model with a number of combinations of the various parameters. Figures 2 displays the results of a calibrating run. The systems are identical with respect to initial value and vulnerabilities. Values increase in step and evolve identically as expected. In each figure, the graph shows the evolution of the values of the 2 systems (lines 1 &2) and of the levels of security (lines 3&4). The dials in the upper left are used to set the initial values of the systems and the vulnerability of system 2. (Increasing vulnerability increases the damage done by attacks.) The switch in the top middle sets the security policy to static (down) or dynamic (up). The sliders on the right were to set other parameters to get a reasonable doubling time. The experiments reported here compare the impact of identical versus different initial values, symmetric versus asymmetric vulnerability, and static versus two dynamic security policies. The remaining figures are summarized in the table below.

Figure	Initial values	Vulnerabilities	Defender Policy
2	same	same	static
3	same	different	static
4	same	different	dynamic: f(V)
5	different	same	static
6	different	same	dynamic: f(V)
7	same	different	dynamic: f(V, A)

Figures 3 and 4 illustrate a situation in which the systems have identical initial values and vulnerabilities but differ in the security policy. Figure 4 must be read carefully because the automatic scaling of the Y axis uses different scales for each line. But it reveals that the static policy is superior over most of life of the simulation.

Careful examination of Figures 5 and 6 and the tables of actual values (not shown) indicate that the naïve dynamic strategy used here is inferior to the static strategy when there are different initial values and similar vulnerabilities. While this is not a definitive result is suggests that dynamic policies should be carefully considered. Further comparison of Figures 2 and 5 and of 2 and 6 suggest that there is value in dispersing the targets. This is consistent with military experience. If we view maximizing the sum of value 1 and value 2 as the objective then in these two cases, splitting the value across 2 hosts gives superior performance.

Figure 7 shows the results of a more complex policy that takes into account previous level of attacks and makes the security proportional to both the current value and previous attack. That result evolves into a rapid oscillation of the security levels without significant improvement in security. The simple interpretation of this result is that rapid responses to attacks may be misplaced if the attackers are also agile. Note that we consider policy changes as cost free, which is almost certainly a strong assumption, one that we plan to relax in due course. As noted in the introduction, one of the key management issues about which we are concerned is that managers don't know what to measure in order to inform their security policy decisions. We see that here in this response.

In general we summarize our findings as follows:

1. Dispersal of value is superior to concentration.

2. With asymmetric vulnerability static security policies are better policies in which security is proportional to value.

3. With asymmetric vulnerability static polices are better than dynamic policies that make security proportional to V*A.

4. Against agile attackers, dynamic polices must be carefully designed.

Much remains to be done. We are engaged is several revisions that we hope will improve this model. First we plan to relax the assumption re use regardless of value. We plan to allow multiple user types with different attitudes toward security. It would be interesting to look at other attacker and defender policies. These are not separable problems, and it remains to incorporate more of the military targeting literature into this effort.

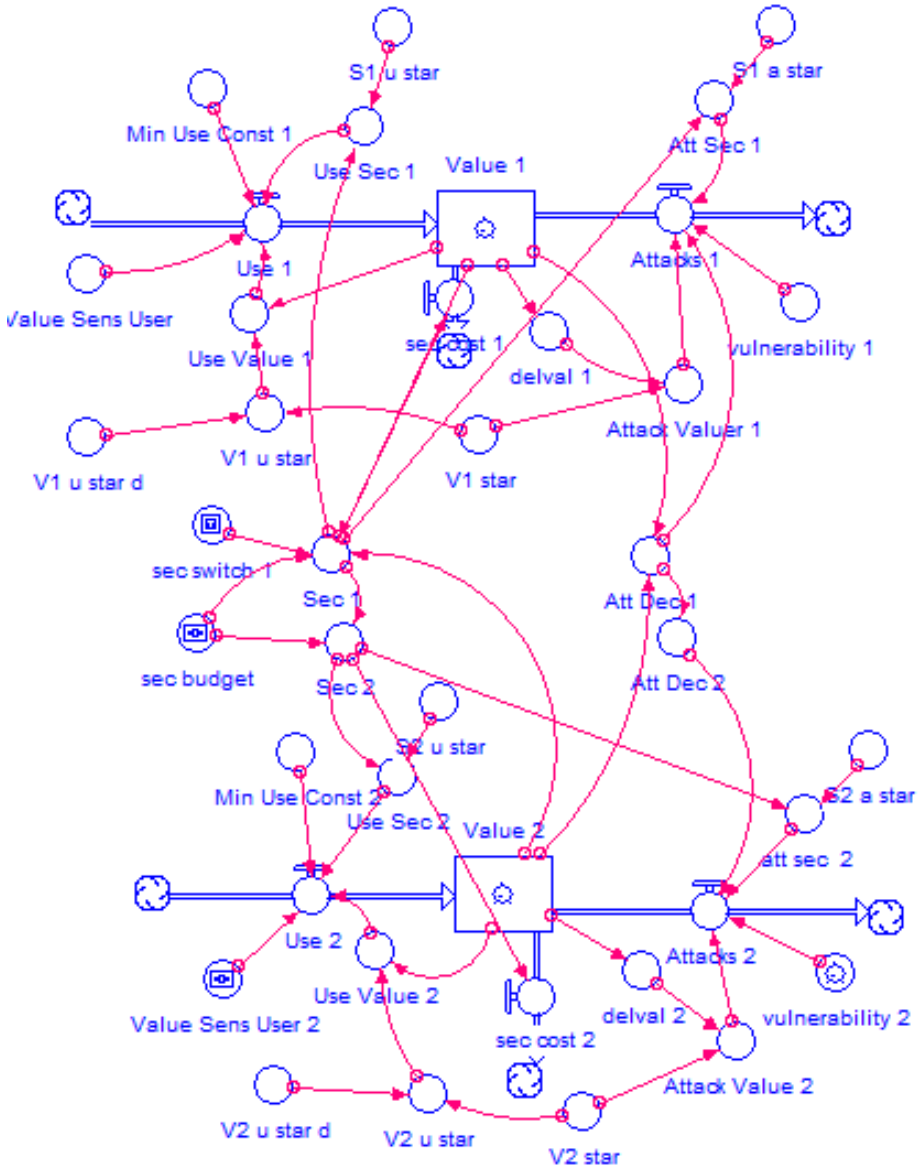

Figure 1
Model

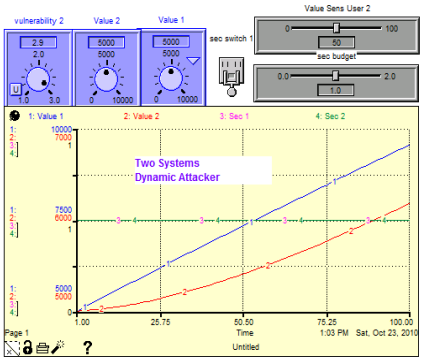

Figure 2: Static Model

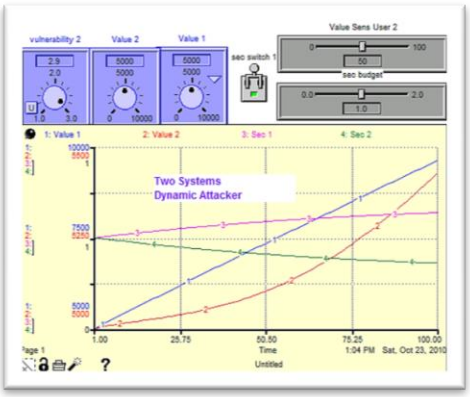

Figure 3: Different Vulnerability

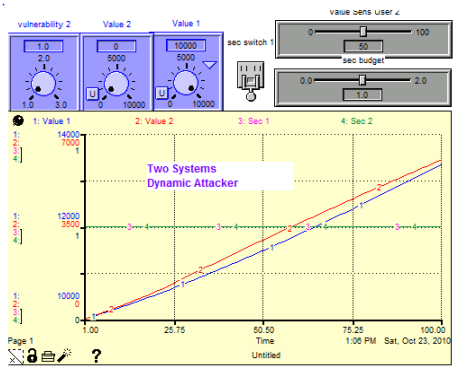

Figure 4: Different Vulnerability/ Dynamic Security

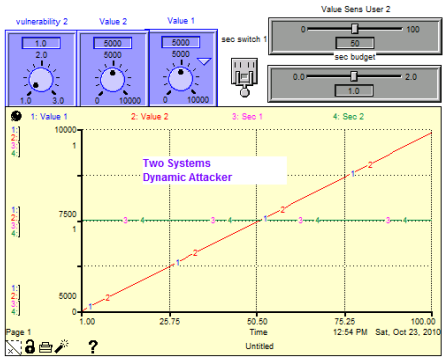

Figure 5: Different Initial / Static Security

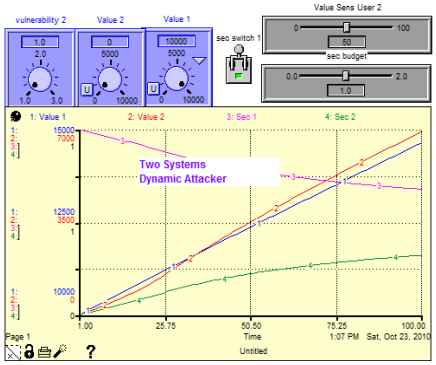

Figure 6: Different Initial/ Dynamic Security

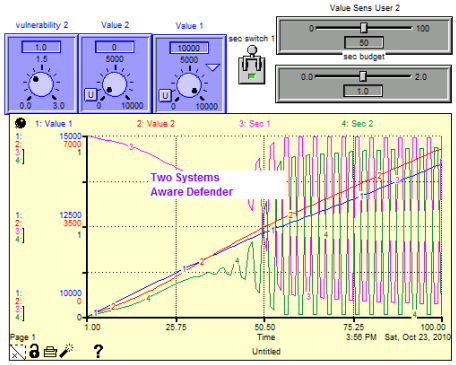

Figure 7: Different Vulnerabilities / Aware Security

REFERENCES

[1] Becker, G.,(1968). Crime and Punishment: An Economic Approach, Journal of Political Economy 78, 169-217.

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

[3] Dutta, A., Roy, R (2008). Dynamics of Organizational Information Security, Systems Dynamics Review 24#3: 349-375.

[4] Forrester, J., (1961), Industrial Dynamics. Waltham, MA: Pegasus Communications.

[5] Holstein, D., 2009. A System Dynamic View of Security Assurance Issues, 42nd 41st Hawaii International Conference on System Sciences.

[6] Martinez-Moyano, I.J, Samsa, M.E., Burke, J.F., Akcam, B.K., 2008. Toward a Generic Model of Security in an Organizational Context:Exploring Insider Threats to Information Infrastructure, 41st Hawaii International Conference on System Sciences.

[7] Pendegraft, N., and Rounds, M., (2007). "A Simulation Model Of IS Security", International Journal of Information Security and Privacy, Vol. 1, Issue 4 July/September pp 62-74.

[8] Peterson, S. and Richmond, B., 1994. ithink: The Visual Thinking Tool for the 90's: Technical Documentation. Hanover, NH: High Performance Systems, Inc.

[9] Sandler, T., and Lapan H., (1988), The calculus of dissent: an analysis of terrorists' choice of targets. Synthese 76:245–261

[10] Schram, A., (2000), "Sorting out the Seeking: The Economics of Individual Motivations", Public Choice, Volume 103, Numbers 3-4 / June, 2000, pp 231-258.

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

[12] Sheeba, P., and Ghose, D., (2005) : "Optimal resource partitioning in a military conflict based on Lanchester attrition models", Proceedings of the 44th IEEE International Conference on Decision and Control and European Control Conference, Seville, Spain, 12-15 Dec 2005