Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

Complex Adaptive Systems, Agent-Based Modeling and Information Assurance

A Burns
Managment and Information Systems, Louisiana Tech University, Ruston, United States., ajb041@latech.edu

Prabashi Nanayakkara
Management and Information Systems, Louisiana Tech University, Rushton, LA, United States., pnc003@latech.edu

James Courtney
Management and Information Systems, Louisiana Tech University, Rushton, LA, United States., courtney@latech.edu

Tom Roberts
Management and Information Systems, Louisiana Tech University, Rushton, LA, United States., troberts@LaTech.edu

Complex Adaptive Systems, Agent-Based Modeling and Information Assurance

A J Burns III
Louisiana Tech University
ajb041@latech.edu

Prabhashi Nanayakkara
Louisiana Tech University
pnc003@latech.edu

James F. Courtney
Louisiana Tech University
courtney@latech.edu

Tom L. Roberts
Louisiana Tech University
troberts@latech.edu

ABSTRACT

Management of information security issues can be viewed as a complex adaptive system because hackers are constantly developing new means of trying to penetrate security systems and access information assets. Organizations must adapt to security threats by updating security procedures and systems, and by training employees in taking precaution security measures to counteract new threats. We present agent-based models that illustrate "phishing" problems, General Deterrence Theory (GDT), and their application to Information Assurance (IA) problems. The agent-based models are developed using Netlogo application, an open-source agent-based modeling system, and are freely available for education and training in IA.

Keywords

Complex Adaptive Systems (CAS), Agent-Based Modeling (ABM), Information Assurance, (IA) General Deterrence Theory (GDT), Phishing, Information Security (IS), NetLogo

INTRODUCTION

Information assurance is ever increasing in importance to the success of organizations of all types. The design of information systems and security mechanisms within them is a complex process. The development of a physical information security system is only the beginning of the overall process. A well-designed system provides a framework within which security is possible, but when a system goes live, human interaction introduces variables that cannot be wholly accounted for in the design and implementation of the system. As information systems become pervasive throughout organizations, many organizations have sought to provide a sanction-based approach to security. This approach comes from criminology and is based on general deterrence theory (GDT) (e.g. Blumstein et al., 1978). Security policies based on GDT are generally restrictive and rely on sanctions to deter users from committing intentional acts that compromise the security of the system or the organization and its information assets.

A pressing issue is the constantly evolving environment in which information assurance must be provided. . Hackers relentlessly search for security weaknesses in operating systems, and devise new viruses, worms, trojan horses and other ways to exploit vulnerabilities. Additionally, new and more sophisticated phishing techniques arise almost daily. Software companies and organizations must continually update operating systems and applications, and keep employees abreast of new phishing techniques and precaution methods against such attacks.

Based on the preceding discussion, it is asserted that the context within which information security (IS) is managed can be viewed as a complex adaptive system that consists of many agents, including: systems developers, IS security analysts, users, managers, and hackers, who interact to produce a dynamic, constantly evolving environment in which behavior is emergent. Regardless of their training levels, employees are still independent agents who must decide how to act when conducting their day-to-day business activities. Therefore, it is proposed that human interaction with security systems can be modeled using an agent-based modeling (ABM) approach within the theoretical framework of complex adaptive systems (CAS).

CAS models are of great interest in IS research, practice, and instruction. These models are unique in their ability to model processes in which characteristics of the system itself emerge. Furthermore, CAS modeling platforms are capable of producing not only meaningful results, but also reporting the results in such a way that is instructive and visually pleasing. Such models can be invaluable in assessing security mechanisms and in reinforcing their importance during Security,

Education, Training & Awareness (SETA) programs of organizations or in ordinary classroom settings. This paper begins with a description of some of the basic principles of CAS and ABM, and then explores their application to information assurance problems using the open-source modeling package known as NetLogo. We show a simple example of a phishing model to introduce NetLogo as a modeling environment, and then describe a second, more complex model based on GDT.

Complex Adaptive Systems Theory

Nobel Prize winner and organizational theorist Herbert Simon **(**1996, p. 183**)** wrote "Roughly, by a complex system I mean one made up of a large number of parts that have many interactions." Simon **(**1996**)** describes three time periods in which there were bursts of interest in studying complex systems. The first followed World War I and resulted in the definition of "holism" and an interest in Gestalts, and a rejection of reductionism. The second followed World War II and involved the development of general systems theory, cybernetics and the study of feedback control mechanisms. The third phase emerged in the latter part of the 20th century and involved the development of catastrophe theory, chaos theory, genetic algorithms and cellular automata. Complex adaptive systems theory (CAS) arose as a natural extension of the aforementioned concepts.

Waldrop **(**1992**)** quotes John Holland, one of the original CAS researchers, as defining a CAS as follows:

> A Complex Adaptive System (CAS) is a dynamic network of many agents (which may represent cells, species, individuals, firms, nations) acting in parallel, constantly acting and reacting to what the other agents are doing. The control of a CAS tends to be highly dispersed and decentralized. If any coherent behavior is to be present/active in the system, that behavior has to arise from competition and cooperation among the agents themselves. The overall behavior of the system is the result of numerous decisions made every moment by many individual agents.

Examples of CAS include economies, social systems, organizations, ecologies, cultures, politics, technologies, traffic, and weather (Dooley, 1997). Choi et al. (2001) analyzed the CAS literature and developed a comprehensive framework of its elements and attributes as shown in Figure 1. The framework consists of three principal elements: internal mechanisms, co-evolution, and environment that are highly interrelated.

In a CAS, agent behavior is typically governed by fairly simple rules that lead to the emergence of "self-organized" patterns of behavior. For example, in a capitalist economy, the tendency of business firms to maximize profits and consumers to maximize utility leads to an efficient allocation of resources. Non-linearity, massive connectivity, and dynamism result in a "rugged environment" for which it is difficult, if not impossible to develop optimal models and solutions.

Co-evolution means that the CAS evolves along with its environment and may cause changes in its environment. Change is constant in CAS and they do not reach a state of equilibrium, but the rate of change varies and may enter a state of quasi-equilibrium. Under severe stress, a CAS may enter a chaotic state and even come to an end, as a firm does if it enters bankruptcy and is dissolved. The notion that CAS must constantly evolve and "live at the edge of chaos" is a prominent feature of the CAS literature. Because of the complexity of CAS, their behavior tends to be non-linear and extremely difficult to predict. As in Chaos Theory, even though the future of a CAS may be non-random, it may not be possible to know the current state accurately enough to predict what future states will be.

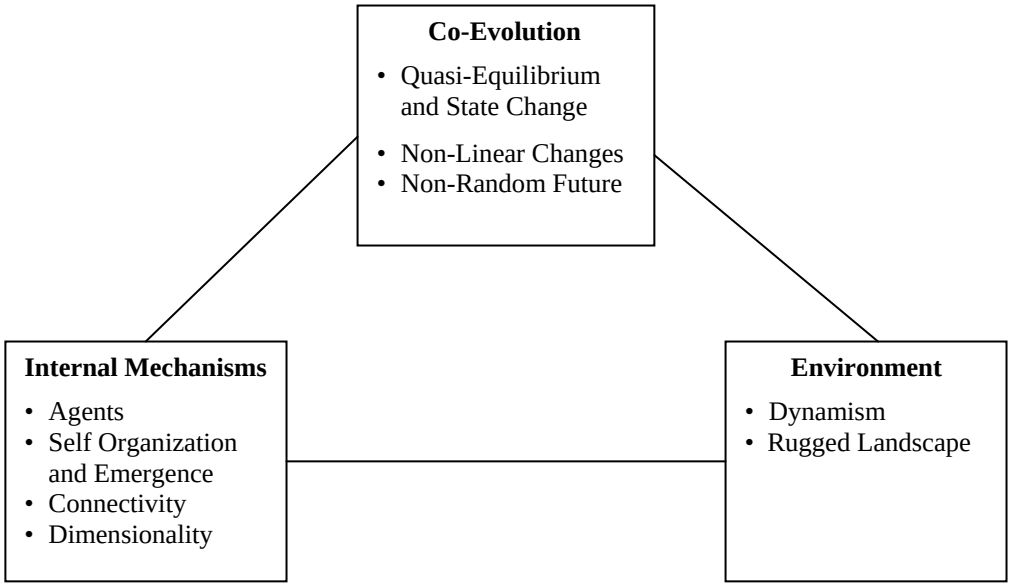

Figure 1: Adapted from (Choi et al., 2001)

Information security (IS) problems may be analyzed as complex adaptive systems. The IS systems exist within complex organizational, social, and governmental environments. Many types of agents operate in an IS environment, including users of information systems, organizational managers, IS designers, and developers, and IS security personnel who safeguard information assets and hackers who try to steal them.

Agent-based modeling (ABM) is widely used to study the behavior of CAS. ABM languages provide the ability to define the various kinds of agents in a CAS, attributes of the agents, and agent interactions. In the following sections, we describe two different models that illustrate how ABM can be used in the context of information assurance. We use NetLogo to develop the models. NetLoto is a simple, widely-used, open-source package which is readily available. The first example, a phishing-attack model developed using NetLogo, is a simple model that illustrates the basic features of ABM.. The second example is a separate, more complex model based on General Deterrence Theory.

A Simple Phishing Model

Central to CAS are the principles of co-evolution and emergence. As such, the dynamism and complexity of relationships among agents and their environment in a CAS make it especially difficult to conceptualize. NetLogo is a modeling platform created by the Center for Connected Learning and Computer-Based Modeling at Northwestern University and is specifically designed for modeling complex relationships among agents (Wilensky, 1999).

In order to illustrate how NetLogo may be used to simulate and study security problems, we have developed an example of a simple, probabilistic model in NetLogo that shows the vulnerability of computer users to phishing attacks. Like most complex adaptive systems, in this simple model, the phishing event ascribes somewhat to chaos theory (Dooley, 1997). There exists a probabilistic relationship between the exposure to a phishing attack and the likelihood of being phished for individual users, but the initial state of security for the user is unknown. The unknown levels are programmed into the model, with unique security levels assigned to users at random when the model is initialized (in this case security levels range between 0 and 100). Additionally, the model specifies a minimum security level required to be immune from the phishing attack. Manipulation of the number of users, number of phishers, and the minimum security level required for immunity manifest the complex relationship between users and phishers in a relatively straightforward manner. The usefulness of the model is limited at the micro-level, where an individual user will either be phished or will remain secure, but at the macro level, the model is very useful because aggregate members of the population will be phished at a probabilistic rate. For example,

Gartner Research estimates that when 57 million U.S. adults were solicited over email with an attempted phishing attack in 2004, nearly 19% took the initial step of clicking the link of the phishing site (Litan, 2004). Furthermore, in one controlled experiment, participants who were not actively suspicious of phishing sites incorrectly trusted phishing websites 40% of the time (Dhamija, Tygar, & Hearst, 2006).

While a model can only be as good as the assumptions on which it is based, as research continues to expand in similar phenomenon, a well-grounded model can be very helpful in studying behavior related to phishing. The primary benefit of modeling security-based probabilistic relationships will be highly conducive for training and instructions. The acting model allows users to visualize the phishing event in a way otherwise impossible. Other studies have sought to represent phishing events in models, but stopped short of providing a 'living model' as is possible with CAS and NetLogo (Jakobsson, 2005).

As seen in the screen shot below (Figure 2A), users are represented as humans and phishers are represented as fish. The Setup button was clicked to initialize the model, but the Go button has not yet been clicked to actually run the model. The number of iterations or "ticks" that the model will be run is set in the "Runs" input box below the Setup button. When a human user becomes compromised, or has been phished, the user turns from grey to red. Users are only phished when they come into contact with phishers while having a state of security that is below the prescribed security level required for a user to be immune from a phishing attack. The minimum security level is set by using the slider bar labeled "Security-Minimum" below the "Runs" box. The desired number of users and phishers are entered in the boxes below the slider bar. The model displays the number of users phished in the box below the slider bar. The simple phishing model can be tailored for specific population statistics and can continue to be modified as research illuminates the true susceptibility statistics in phishing attacks. The model in Figure 2A and 2B is set for 100 users, 10 phishers, and 100 ticks.

Users and phishers are agents (called turtles in NetLogo) that can move. The window in which the agents move is divided into a grid, the cells of which are called "patches." During the initialization process, the desired number of phishers and users are randomly assigned to patches, and users are assigned a personal security level. Phishers and users then move about the grid during each tick of the run. If a user and a phisher land on the same patch, and the user's personal security level is below the set minimum required for immunity, then the user's color changes to red as a result of the phishing attack. Figure 2B shows the results after 100 ticks. Thirty-seven users have been phished. Suppose we have security training that reduces the required minimum security level to 35 for an individual to be immune from a phishing attack. The results are shown in Figure 2C and 23 users have been phished.

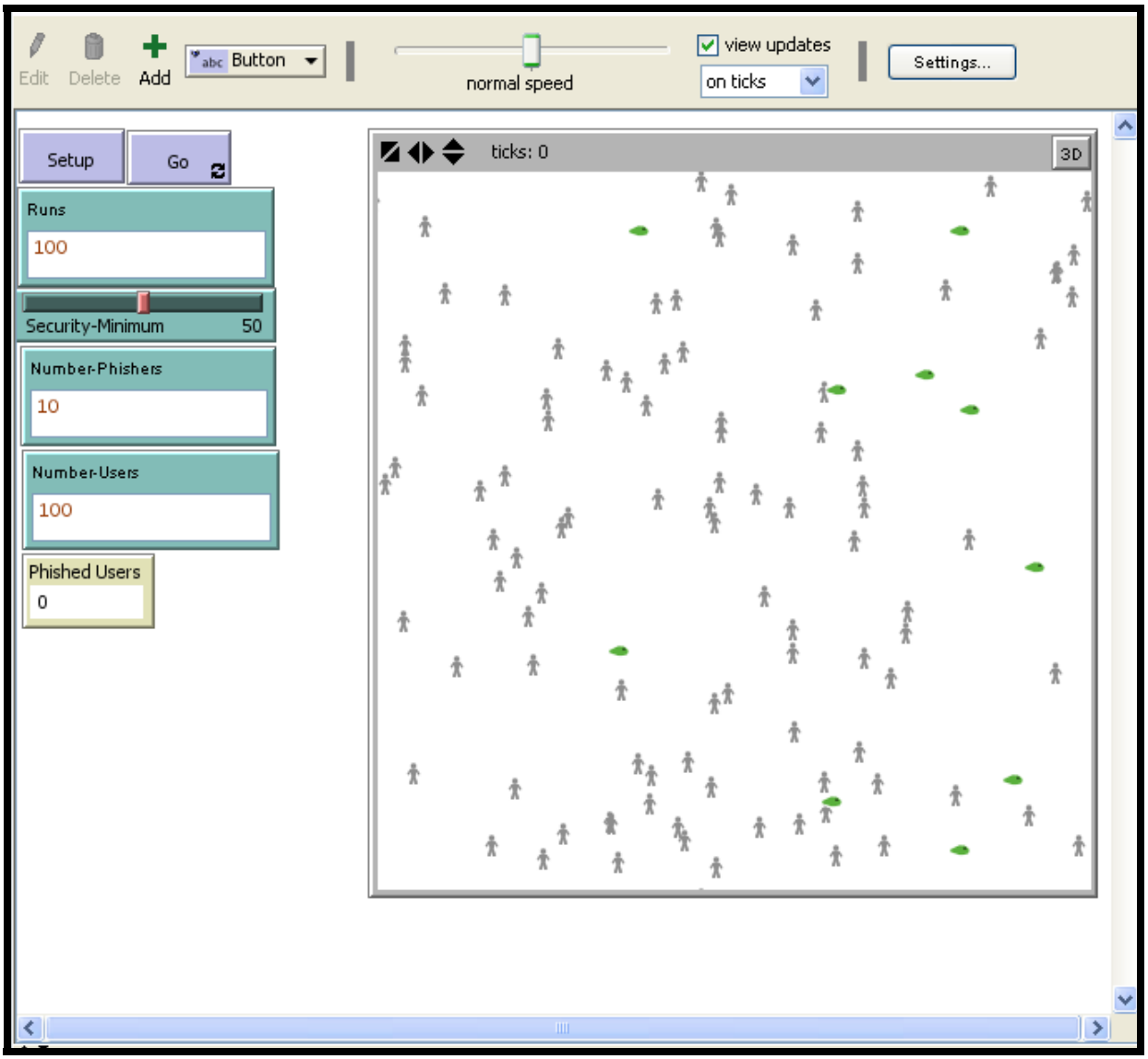

Figure 2A. Phishing model

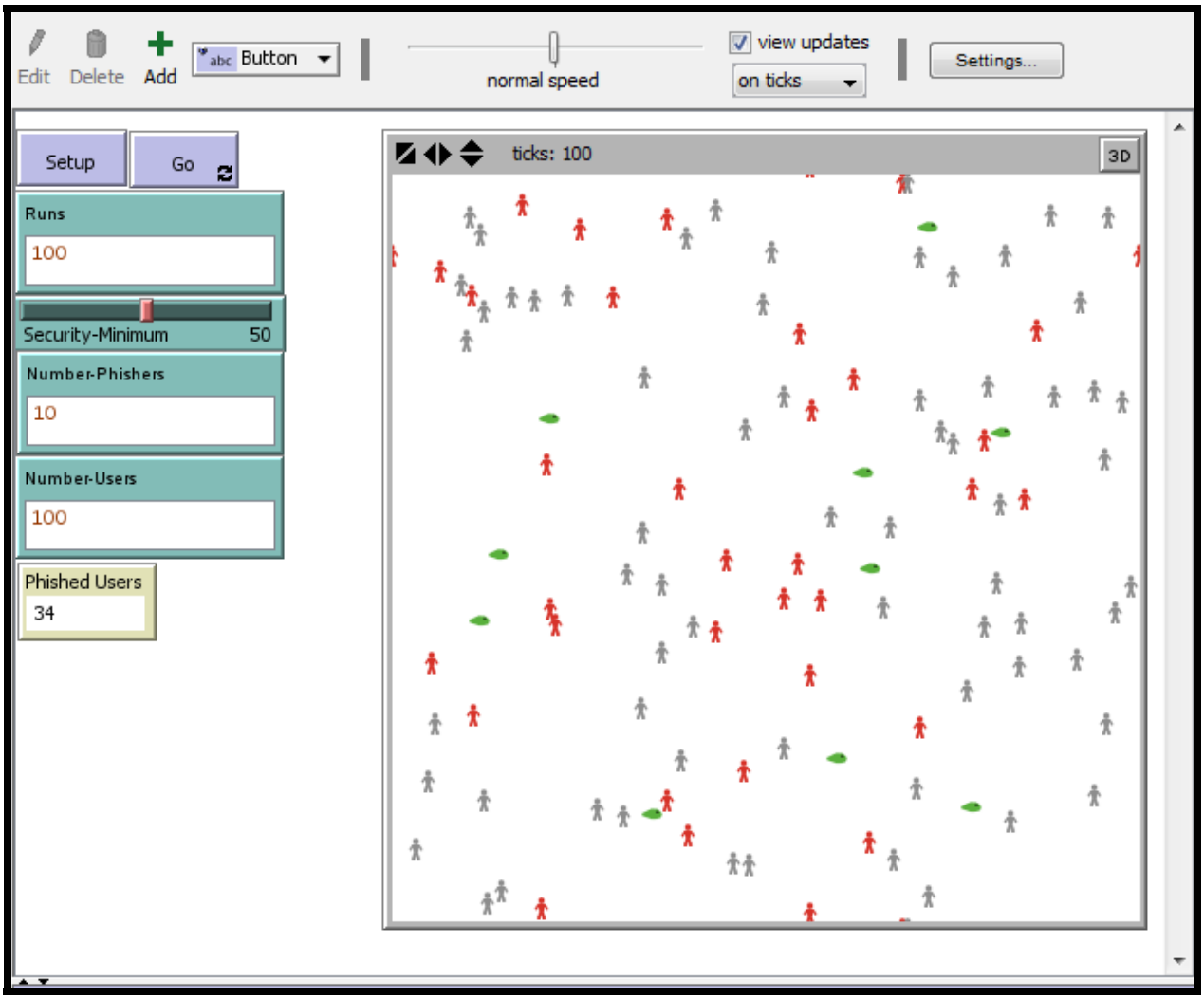

Figure 2B. Original assumptions of 100 runs, 10 phishers, 100 users and 50 security minimum

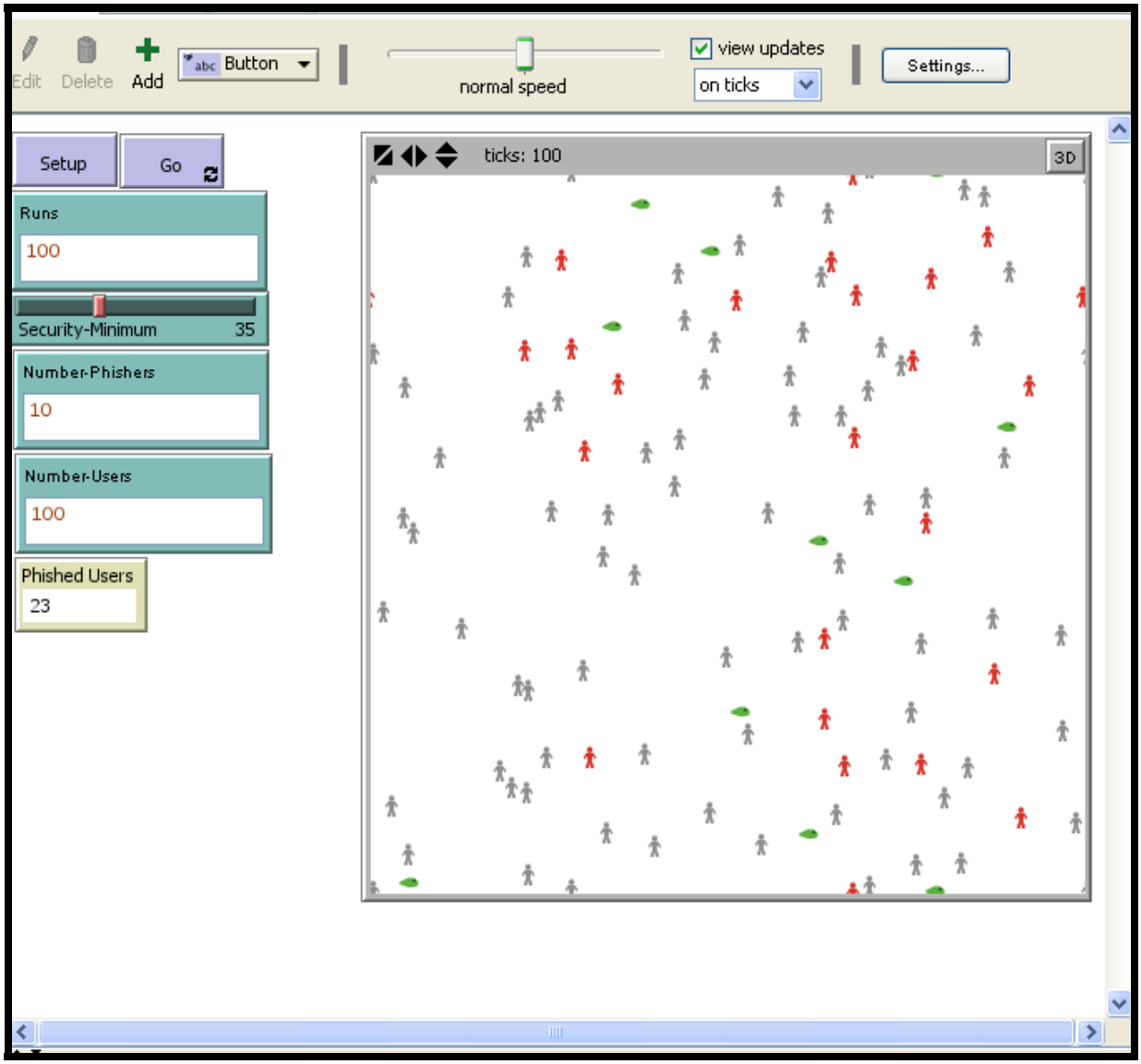

Figure 2C. Security minimum set at 35.

Complex Theoretical Models

In NetLogo, it is also possible to go beyond simple models and demonstrate fairly complex theoretical models. An advantage of using NetLogo for modeling complex adaptive systems is the ability to use the interface to make significant changes in the assumptions of the model in order to analyze system behavior under various conditions. The output is especially useful for comparing theories which seek to explain a similar dependent variable such as motivation to conform to security policies. The actual motivated activities need not be similar, and in fact, the ability to show alternate security views in similar models creates a unique opportunity to compare the results of differing security paradigms. Next a complex model is presented that has been fitted to model GDT toward the goal of exhibiting the overall security in a sanction based/reactionary security paradigm.

General Deterrence Theory

An organization using a deterrence security model imposes sanctions, penalties, disincentives, or any combination of them. Straub (1990) asserts that GDT's disincentives and sanctions against IS breaches or deviant behavior, effectively hinder individuals from such involvements. GDT has been applied in preventing deviant acts in various areas, such as drug abuse

(Anderson et al., 1977; Meier and Johnson, 1977), drug sales (Miller and Anderson, 1986), employee theft (Hollinger and Clark, 1983; Miller and Anderson, 1986), school delinquency (Jensen et al., 1978), school misbehavior (Pestello, 1989), tax evasion (Miller and Anderson, 1986; Wenzel, 2004), underage drinking (Paternoster and Iovanni, 1986), and vandalism (Paternoster and Iovanni, 1986).

Our model includes three organizational disincentives that criminology research has shown to be important in determining potential immoral activities(Gray and Martin, 1969):

(1) Certainty of sanction or the perceived likelihood of the perpetrator being caught in a deviant act (Tittle and Rowe, 1974; Silberman, 1976; Straub, 1990; Antia, Bergen, Dutta, and Fisher, 2006),

(2) Severity of sanction or the gravity of the ramifications a violator faces for such involvement if caught (Silberman, 1976; Straub, 1990; Antia et al., 2006), and

(3) Celerity of sanction or swiftness in punishing the perpetrator once caught (Antia et al., 2006).

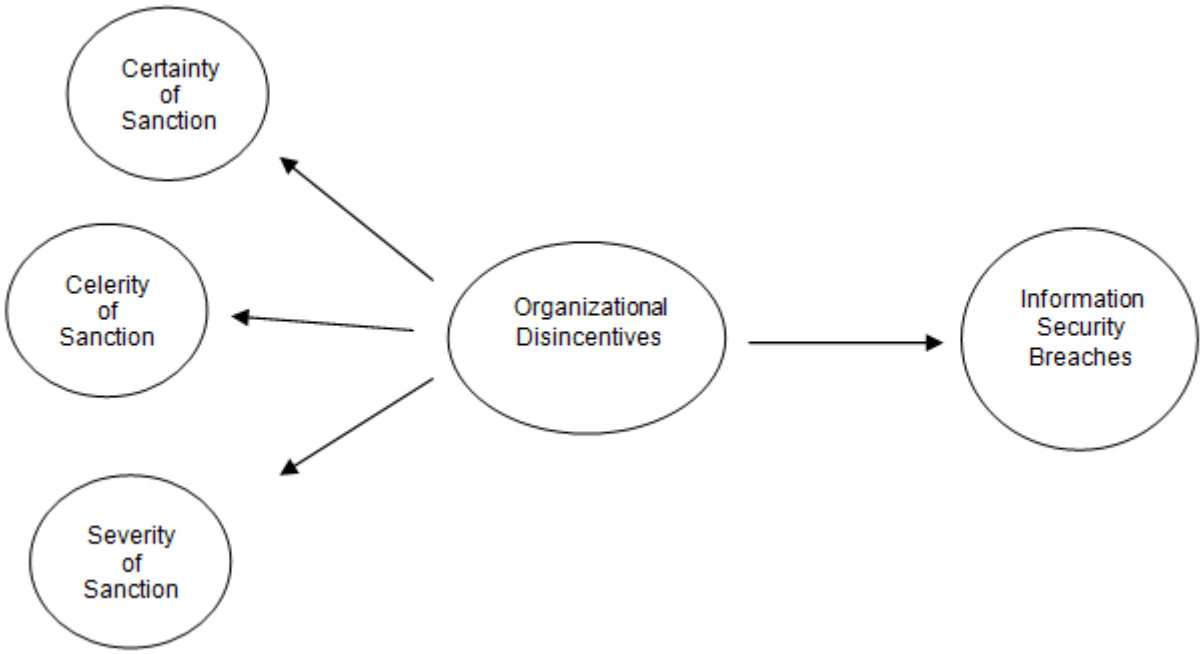

Figure 3: General Deterrence Theory Model

GDT Model- The GDT model in NetLogo also utilizes the interaction of the environment (patches) and agents (turtles) in order to model the emergence of organizational security. In the GDT model, the behavior space which is made up of patches can be viewed as a security grid for an organization. Each patch is either secure or insecure. Those patches which are secure are colored blue, while insecure patches are black. In the GDT model, the initial state of patch security is assigned randomly according to the "Physical-Security" slider. In the two GDT models shown below, the "Physical-Security" slider is set to 90, which stipulates to the model that each patch has a 90% likelihood of being secure (blue) initially. The agents have characteristics which are personal security levels. The base-level personal security levels are assigned according the "culture" slider, which can be set as a number 1-100. The culture number represents the probability that an individual in the model will have an adequate level of security, denoted by "MinimumSecurity". Those individuals with a security level lower than the minimum are insecure individuals and are colored red. Individuals with adequate security are colored green. Insecure individuals impact their environment negatively and make the patches they come in contact with insecure (black). The patches may also become insecure from some outside threat, which is modeled probabilistically by the "New-Risks" slider. At every increment each patch has a probability of becoming insecure according to the level on the slider (i.e. when the slider is set to three, at each increment in the model every patch has a three percent probability of becoming insecure).

In a deterrent model with a reactionary paradigm, the users are thought of solely as threats and when security is breached a centralized IT reaction is deployed. In the GDT NetLogo model, when the "Reactionary-Security" switch is in the 'on'

position and the overall security level is below the "ReactLevel" slider, the model employs a reaction which returns the system to its initial security state. This induces the wild swings in the security level in the security plots. The level of response to each of the three appeals affects the rate at which the system becomes insecure.

Figures 4A and 4B show that by increasing the believability of the certainty, severity, and celerity of the deterrent, the rate at which the system grew insecure was reduced. In figure 4A the believability of the certainty, severity, and celerity was assumed to be only 50%, while in figure 4B, the levels of certainty, severity, and celerity were set to 100%. Over the same period (20 ticks), two fewer security reaction was necessary to maintain the same level of security in the model with 100% levels of Certainty, Severity, Celerity (Figure 4B). Therefore, with a reactionary paradigm such as GDT, the rate at which the organization reaches insecurity can be decreased substantially by increasing the appeals to the three aspects of GDT.

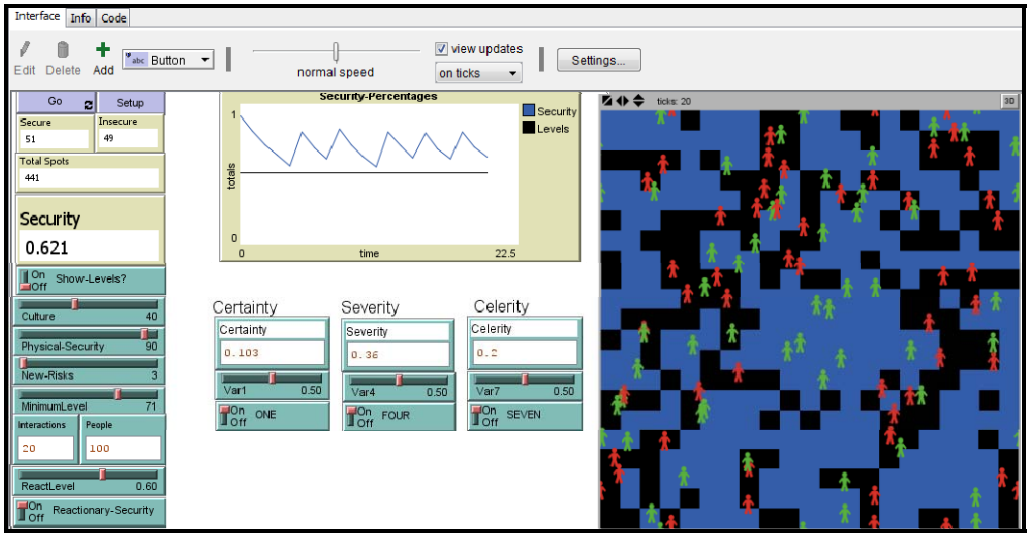

Figure 4A: GDT Model - 50% Levels

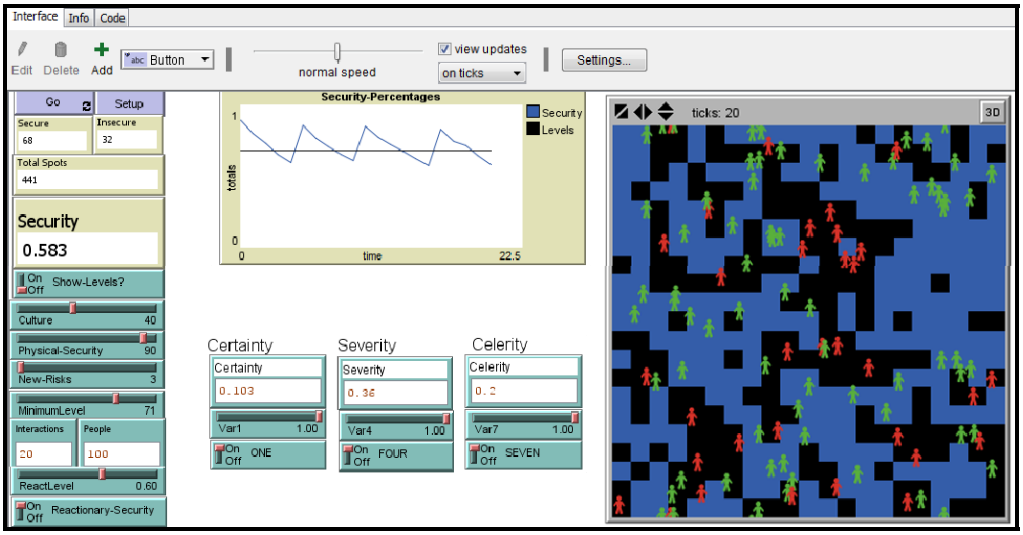

Figure 4B: GDT Model - 100% Levels

Discussion

Solving information assurance (IA) problems is a mission comprised of an array of interacting agents, including: managers and information security (IS) analysts who are responsible for protecting an organization's information assets, users who

access, manage and use information assets, and hackers who attempt to penetrate security and steal information assets. This is a dynamic environment in which hackers continually develop new and innovative ways to penetrate security systems, and organizations devise measures to counter them. This situation constitutes a complex adaptive system with organizational agents and hackers responding to each other's moves while the environment co-evolves and emerges through this adaptive behavior.

CAS, agent-based modeling, and IA are simulated to demonstrate the curbing of IS breaches based on elements of GDT. By using NetLogo, an open source CAS simulation software package, this paper presents models of IS breaches and IA based on an individual's security-minimum and reactive GDT levels in a logical and compelling manner. As simulated in the two models, simple-phishing and GDT, the higher security levels in individuals and organizations, denote lower amount of IS breaches. The simple phishing-model illustrates that when the user security-vulnerablility levels are higher, IS breaches are higher and vice versa. The GDT model illustrates that when reaction levels, physical security, and minimum levels are high, the organization is more adept at deterring IS breaches. One conclusion which can be drawn from these models is that in order to maintain higher security levels, an organization should regularly conduct SETA programs to reinforce awareness of the need for vigilance regarding the protection of information assets

REFERENCES

1. Anderson, L.S., Chiricos, T. G. and Waldo, G. P. (1997) Formal and Informal Sanctions: A Comparison of Deterrent Effects, *Social Problems*, 25, 1, 103-114.
2. Antia, K.D., Bergen, M. E. Dutta, S. and Fisher, R. J. (2006) How Does Enforcement Deter Gray Market Incidence?, *Journal of Marketing*, 70, 92-106.
3. Blumstein, A., Cohen, J., & Nagin, D. (1978). Deterrence and incapacitation. Washington, DC: National Academy of Sciences.
4. Choi, T. Y., Dooley, K. J. and Rungtusanatham, M. (2001) Supply Networks and Complex Adaptive Systems: Control Versus Emergence, *Journal of Operations Management*, 19, 3, 351-366.
5. Dhamija, R., Tygar, J. D. and Hearst, M. (2006) Why Phishing Works, *Proceedings of the SIGCHI conference on Human Factors in computing systems*
6. Dooley, K. J. (1997) A Complex Adaptive Systems Model of Organization Change, *Nonlinear Dynamics, Psychology, and Life Sciences*, 1, 1, 69-97.
7. Gray, L.N. and Martin, J. D. (1969) Punishment and deterrence: Another analysis of Gibbs' data, *Social Science Quarterly*, 50, 2, 389-395.
8. Hollinger, R.C., and Clark, J. P. (1983) Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft, *Social Forces*, 62, 2, 398-418.
9. Jakobsson, M. (2005) Modeling and Preventing Phishing Attacks, *Lecture Notes in Computer Science*, 3570, 1-18.
10. Jensen, G.F., Erickson, M. L. and Gibbs, J.P. (1978) Perceived Risk of Punishment and Self-Reported Delinquency, *Social Forces*, 57, 1, 57-78.
11. Litan, A. (2004) Phishing Attack Victims Likely Targets for Identity Theft, *Gartner Research*.
12. Meier, R.F. and Johnson, W.T. (1977) Deterrence as Social Control: the Legal and Extralegal Production of Conformity, *American Sociological Review*, 42, 2, 292-304.
13. Miller, J.L. and Anderson, A. B. (1986) Updating the Deterrence Doctrine, *Journal of Criminal Law and Criminology*, 77, 2, 418-438.
14. Paternoster, R. and Iovanni, L. (1986). The Deterrent Effect of Perceived Severity: A Reexamination, *Social Forces* 64, 3, 751-777.
15. Pestello, F.G. (1989) Misbehavior in High School Classrooms, *Youth & Society*, 20, 3, 290-306.
16. Silberman, M. (1976) Toward a theory of criminal deterrence, *American Sociological Review*, 41, 3, 442-461.
17. Simon, A. H. (1996) The Science of the Artificial, 3rd edition, MIT Press, Cambridge Mass.
18. Straub, D. W. (1990) Effective IS Security, *Information Systems Research*, 1, 3, 255-276.
19. Tittle, C.R. and Rowe, A. R. (1974) Certainty of Arrest and Crime Rates: A Further Test of the Deterrence Hypothesis, *Social Forces*, 52, 4, 455-462.
20. Waldrop, M. M. (1992) Complexity: The Emerging Science at the Edge of Order and Chaos, 1-380.
21. Wenzel, M. (2004) The Social Side of Sanctions: Personal and Social Norms as Moderators of Deterrence, *Law and Human Behavior*, 28, 5, 547-567.
22. Wilensky, U. (1999) NetLogo (and NetLogo User Manual), Center for Connected Learning and Computer-Based Modeling, Northwestern University. http://ccl.northwestern.edu/netlogo.