Towards Modeling Factors that Enable an Attacker

Daniele Vernon-Bido
Dept. of Modeling, Simulation
& Visualization Engineering
Old Dominion University
1300 Eng. & Comp. Sciences
Norfolk, VA 23529, USA
dvern001@odu.edu

Jose J. Padilla
Virginia Modeling Analysis and
Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
jpadilla@odu.edu

Saikou Y. Diallo
Virginia Modeling Analysis and
Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
sdiallo@odu.edu

Hamdi Kavak
Dept. of Modeling, Simulation &
Visualization Engineering
Old Dominion University
1300 Eng. & Comp. Sciences
Norfolk, VA 23529, USA
hkava001@odu.edu

Ross J. Gore
Virginia Modeling Analysis and
Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
rgore@odu.edu

ABSTRACT

This paper presents an initial baseline model of factors that give rise to an attacker. It explores the impact of successful rate of attack and social learning on the decision to become an attacker. The model utilizes rational choice theory, routine activity theory, social learning theory, and perceived behavioral control from the theory of planned behavior to examine factors that moves an individual from user to attacker. An agent-based model is used to depict the effect of interactions of users and attacks of all users, successful and unsuccessful, have on an individual's decision to become an attacker. Preliminary results suggest that opportunity has a stronger influence than the rate of successful attacks or the size of the associated group.

Author Keywords
Cyber-crime; agent-based modeling; simulation

ACM Classification Keywords
I.6.1 SIMULATION AND MODELING

1. INTRODUCTION

Research on the behavior of cyber attacks is lacking primarily because it is hard to identify and access hackers. Despite these difficulties, the International Federation for Information Processing (IFIP) Work Group believes that "… gaining a rich understanding of hacker behavior could lead to native theories in information security research field that could have a profound impact for a number of related academic disciplines [8, p. 93]."

One area of study that is beneficial is research on the factors involved in an individual's decision to attack. Current research [9, 12, 13, 15] on hackers suggests that there is a community or social structure that provides the basis for learning. Xu et al. [25] acknowledge that association is an enabler but states that in the early stages tolerance of the behavior is also a strong component. Social learning and successful attacks (i.e. attacks that do not generate repercussions) are both factors. However, there is no indication of which factor is more influential.

In this paper we will use agent-based simulation to compare three factors, group size, success rate and opportunity, to determine which has the greater influence. We create a baseline model of a connected group of users to explore the number of individuals that move from being willing to attack to actively seeking to attack.

The paper is organized as follows. Section two provides background information on hackers and crime theories used to study hackers. In section three there is a description of the model. Section four reviews the results produced from the simulation. A discussion follows in section five and section six concludes the paper.

2. BACKGROUND

In depth research on computer hackers is lacking primarily due to inaccessibility to data. Several researchers have, however, made significant attempts. Chantler [6]

SummerSim, 2016 July 24-27, Montreal, Quebec, Canada

characterizes hackers from qualitative data gathered using online surveys, interviews and site monitoring. He determines that hackers are self-motivated, intensely curious individuals about systems but had decidedly skewed ethical boundaries. Hollinger [11] determines that there is a likelihood of committing a computer crime if an individual associated with others that commit computer crime.

Association appears to be a prominent attribute of cyber attackers. Several researchers [9, 12, 13, 15] have studied the social networks and communities of hackers. Jordan and Taylor [15] use interviews to gain insight into the "imagined community" of hackers. Holt [12] confirms [15] assessment of the hacker social network. He finds a subculture that exists, on-line and off-line, of sharing information, hierarchical positioning, demonstrating commitment and mastery, and recounting exploits. Other researchers have classified hackers by their skill level [6, 19]. However, a classification does not aid in determining the factors that give rise to the act.

In the absence of theories specifically aimed toward hackers, researchers often employ criminology theories some of which are Rational Choice Theory [5], Social Learning Theory [2], and Theory of Planned Behavior [1]. Rational Choice Theory is an economic based theory that assumes we make rational decisions based on expected utility – cost to benefits ratio. Rational Choice Theory is the basis for several studies of computer hackers [14, 18, 20, 24] as it provides insight into behavioral decisions. However, humans are not purely rational. They are subject to a bounded-rationality [21] – that is, they do not have full knowledge or the capacity to account for all possibilities. Further, they are subject to emotions, social learning and norms, and individual propensity. Tibbets and Gibson [23] surmise that deviant behavior is strongly related to rational choice measures and individual propensity – the likelihood of acting on an impulse based on an individual's level of self-control.

Hu et al. [14] use Rational Choice Theory to study the effects of deterrence on users that might choose to commit information security policy violations in the workplace. Their conceptual model factors in the individual's moral beliefs – their sense of right and wrong – and their level of self-control, which they refer to as propensity, and the perceived deterrence. They conclude that perceived benefits, not the cost-benefit ratio or the perceived deterrence, is the dominant influence. Beck and Ajzen [4] show that perceived behavioral control is strongly correlated to intention to behave dishonestly.

We postulate that social association, perceived benefits, and perceived behavioral control determine the factors that moves an individual to become a hacker.

3. THE MODEL

Sokolowski et al. [22] use agent-based models to study of individuals that become an insider threat. In their model, Epstein's Agent_Zero [10] structure is implemented to examine the effect disgruntlement, rational behavior, and the disposition of others has on the agent's own disposition. Using their example, we examine the likelihood of any user, not just an insider, converting to an active attacker. We use the term attacker to denote that we model an individual that seeks to attack rather than a hacker, which to some might encompass attitude and motivation. Further, we advance the model to include the attack.

We model the interaction of users to compare the effect of group size, attack success rate, and rate of opportunity on the migration to attacker and the number of attacks. The model represents a group of loosely connected users that are predisposed to commit cyber-crime. They share access to information/knowledge. Social Learning Theory suggests that individuals acquire knowledge and patterns of behavior through experience or observation [3]. Social learning not only improves skills and techniques, but also reinforces drive, motivation and rationalization of behavior [2]. This environment provides for social learning to take place. The theories discussed drive behaviors of the users. Theories link to attributes and behaviors are given in Table 1.

Theory	**Attribute or Behavior**
Social Learning Theory	Social component equation: users gain experiential confidence from the social connection with others.
Routine Activity Theory	Users attack only after reaching a level of motivation and an opportunity presents itself
Perceived Behavioral Control (from Theory of Planned Behavior)	Threshold that a user's Experiential Confidence (XC) must cross for the user to believe he can successfully attack
Rational Choice	Cognitive component

Table 1: Theories applied to attributes and behaviors in the model.

Our model design uses Epstein's theoretical Agent_Zero [10]. Users in the model are limited to only those that have the attitude or propensity to commit cyber-crime. The perceived benefit is represented by level of success the user senses in the group. This is the cognitive component of the model. The cognitive probability (P) is the local number of successful attacks divided by the local number of attempted attacks. Epstein uses the Rescorla Wagner equation to represent the affective component.

$$\frac{dv_i}{dt} = \alpha\beta(\lambda - v_i)$$

Where α and β represent the prominence of conditioned stimulus and unconditioned response and λ represents the learning rate. This equation, in our model, simply represents a learning curve.

The disposition of a user at time t is then

$$D_i(t) = v_i(t) + P_i(t)$$

Next, we consider the social learning component. The social component, taken from Agent_Zero, is as follows

$$D^{tot}{}_i(t) = \sum_{j \neq i} \omega_{ji} D_j(t)$$

ω_{ji} is the weighted strength of influence between users j and i.

Table 2 provides a definition of our agent and its initial values. Each user is randomly assigned a threshold value. The user's affective rate is calculated using the Rescorla Wagner equation given above. For the cognitive component for each agent *i* at time *t*, $P_i(t)$, the user compiles the ratio of successful attacks, *S*, to total attacks, *A*, of other users to which he is linked. Links are given by matrix *q* where q_{ji} is 1 if there is a link, 0 if there is not a link.

$$P_i(t) = \frac{\sum_{j \neq i} q_{ji} S_j}{\sum_{j \neq i} q_{ji} A_j}$$

The user's individual disposition is the sum of the affective and the cognitive components. The model uses Epstein's D^{tot} equation above to determine XC.

Agent Type	User	
Agent Attributes	Learning rate	0.001
	XC	0
	Perceived Benefits Threshold	*Uniform* (0.0-1.5)
	# of Attacks	0
	# of Successful Attacks	0
	XC at last attack	0
Agent Behaviors	Attack	
	Gain/Lose Experiential Confidence	

Table 2: Agent definition and initial values.

The decision to attack is an individual threshold for each user. Users chose to become attackers when their XC exceeds their threshold for perceived benefits. Users gain confidence individual learning, social learning, but lose confidence when an attack is unsuccessful.

Users that have chosen to attack cannot do so until an opportunity presents itself. This assumption comes from the Routine Activity Theory [7] – crime can only occur when a motivated offender meets with a suitable target in the absence of a capable guardian. An individual with the intention to attack is the motivated offender. Opportunity, the suitable target, is represented in the model as a probability of occurring at any time. The capable guardian is a perceived deterrence. In this model, the deterrence is the lack of experiential confidence to successfully executing the task (i.e. lack of perceived behavioral control or experience).

The dependent variable in this model is the decision to become an attacker. The independent variables are group size (size ranges from 2 to 50), success rate, and opportunity. XC is initialized to 2 representing an individual with limited knowledge of the system. The threshold is a random real number between 0 and 1.5. The maximum affective value (λ) is 1. The learning rate is 0.001. α and β are 1. The weight of the social component is 0.3. Individual disposition and opportunity are randomly selected binaries. Success or failure of an action and the disposition of users are drawn from probability distributions. The duration of the model execution is 1095 time steps. This represents one day per time step for a period of 3 years. Figure 1 shows the flow of the simulation.

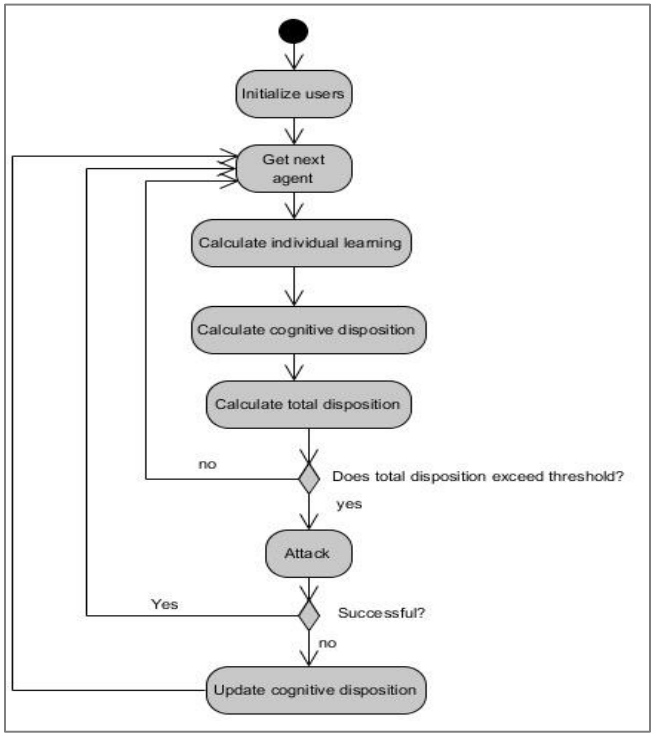
Initialize users
Get next agent
Calculate individual learning
Calculate cognitive disposition
Calculate total disposition
no
Does total disposition exceed threshold?
yes
Attack
Yes
Successful?
no
Update cognitive disposition

Figure 1: Activity flow diagram of the model.

The assumptions of the model are as follows: users are only aware of the successes and failures of other users with whom they share a link; and all users equally influence a user.

We execute the simulation 30 times with the success rate set at 0.5, the group size at 50 and the rate of opportunity at 0.5 to determine the number of runs necessary for a confidence level of 95%. The average number of attackers is 32. The standard deviation (σ) for number of attackers for this sample is 3.216 and the standard error (SE) is 0.578. The following formula determines the number of runs necessary for a confidence level of 95%

$$Runs = 1.96(\frac{\sigma}{SE})^2$$

There are 115 iterations required for the desired confidence level. Further, there are an infinite number of combinations possible with the three dependent variables. To reduce the computational load, we use Latin Hypercube Sampling (LHS) [16] to select 100 combinations for testing. Figure 2 details the sampling of parameters selected from the sample space for runs of the experiment.

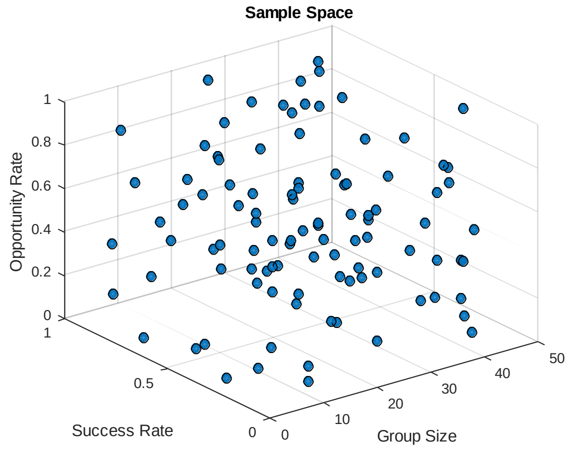

Figure 2: Selected parameters from sample space using LHS.

4. RESULTS

We examine the number of attackers as a ratio of the group size. Figure 3 shows that the ratio of attackers to total group is relatively constant with a mean of 0.642 and a 95% confidence interval of 0.636 to 0.648. This result is not unexpected despite each individual only being able to initiate a single link. The group is predisposed toward this action.

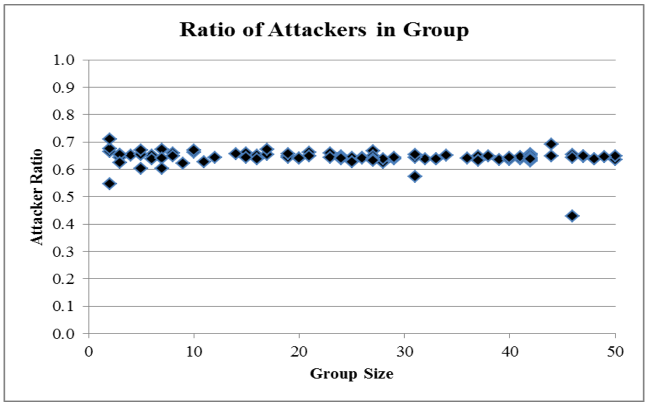

Figure 3: Ratio of attackers to group size.

However, as figure 4 demonstrates, the number of attacks per person varies greatly. While the overall mean number of attacks approximately 206.6, the variance is 15919.4. Furthermore, there does not appear to be any direct correlation between the group size and the number of attacks per person.

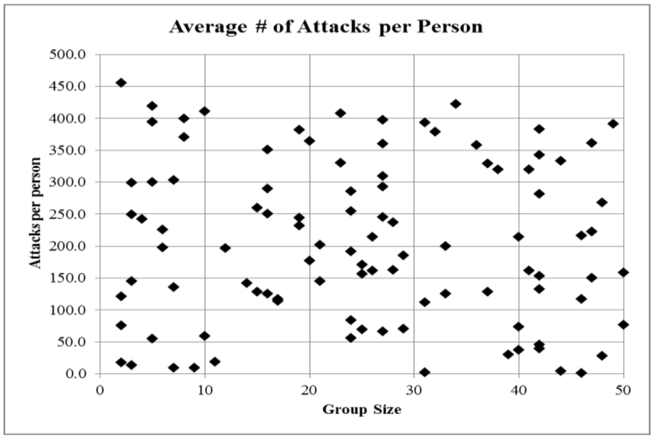

Figure 4: Average number of attacks per person.

Table 3 clusters the data into groups to examine further the relationship of group size to average number of attacks per person. This still fails to produce any meaningful correlations. We therefore conclude that group size is not a factor that drives the number of individuals that migrate to active attackers or the number of attacks committed by those individuals.

	# of Samples	**Mean**	**Variance**
Less than 11	20	213.28	22971.63
11 to 20	16	211.93	10611.00
21 to 30	24	210.61	10912.04
31 to 40	15	208.25	21610.04
41 to 50	22	190.31	16676.46

Table 3: Mean and variance of samples grouped by 10.

We next compare the two remaining factors – success rate and opportunity – with the ratio of attackers and number of attacks. Group size does not determine the attack rate for an individual. However, a comparison of attack rate per person with the other independent variables in Figure 5 shows a direct linear correlation between the attacks per person and the level of opportunity. Opportunity appears to be the most significant factor in the proliferation of attacks; individuals that become inclined to attack need only an opportunity to present it. Success rate, conversely, appears to have no effect. This suggests that the lack of success or the greater risk of failure is not a deterrent to the crime.

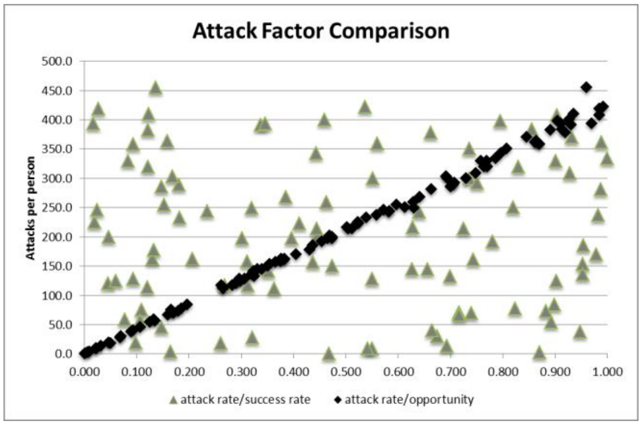

Figure 5: Average number of attacks/person by success rate and opportunity.

It also confirms that traditional theories such as deterrence theory and rational choice may need to be altered to address cyber-crime.

5. DISCUSSION

The current model represents a group of users that is predisposed to become attackers. It examines the size of the group, the success rate of group members, and the number of opportunities that present themselves. The goal is to improve our understanding of the factors that move an individual to attacker from predisposed user.

Cybersecurity has benefitted from significant advances in the technology. Firewalls, anti-virus, and intrusion detection, for example, have made operating in cyberspace safer. However, we ultimately must address the human component of cyber-attacks. Why do people attack? Understanding the motive and the timing should ultimately improve our ability to prevent or respond making systems more resilient.

The model is intentionally simplistic to allow for the isolation of factors. Further, it is only intended to generate theories. There is no empirical validation at this point. The purpose of this exercise is to begin to review what are the drivers of an attack, how do this drivers work in combination and what means is available to limit attacks in the future.

In this model, we began with a population that was predisposed to attack. Studies of insider threat with respect to system sabotage show that there are often behavioral precursors that indicate a user might be predisposed to attack [17]. Does this hold for all types of attackers or is it isolated to insider threat? Is there a means to screen for this predisposition? Literature on hackers indicates that there are only a limited number of attackers capable of creating truly unique hacks [12, 13]; others copy code shared through websites, blogs, etc. Can we estimate the predisposed population through examining the number of unique visitors to various hacking websites?

The goal for the future is to build a model that allows us to determine the combination of factors that gives rise to attackers and insider threats. We anticipate expanding on the baseline model validating each segment before adding an additional factor. The ultimate aim is to create a profile that allows us to recognize and alter the conditions that give rise to attackers.

6. CONCLUSION

In this paper we presented a model that compared three factors – group size, attack success rate, and opportunity – that potentially contributed to migrating a predisposed user to an active attacker. We employed the theory of planned behavior, rational choice theory, social learning theory, and routine activity theory. We used the concepts developed in [10] to incorporate the social, cognitive, and affective disposition in the decision process. We determined that of the three factors, opportunity was the only factor that had a direct linear correlation with the number of attacks.

The work presented is a preliminary study to establish the variables that will help identify and eventually mitigate the factors that influence cyber attacks. The research on the spectrum of system users to cyber attackers has been limited to date. We believe this is an important field of research that has to potential to yield significant and impactful results.

Acknowledgment

This material is based on research sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) under agreement number FAB750-15-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

Disclaimer

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) or the U.S. Government.

References

1. Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior* (pp. 11-39). Springer Berlin Heidelberg.
2. Akers, R. L. (1977). Deviant behavior: A social learning approach.
3. Bandura, Albert. (1977). "Social learning theory." 305-316.
4. Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. *Journal of research in personality*, *25*(3), 285-301.
5. Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy 76*, 169−217.
6. Chantler, N. (1996). Profile of a computer hacker. *Florida: infowar*.
7. Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.
8. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90-101.
9. Décary-Hétu, D., and Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175.
10. Epstein, J. M. (2014). *Agent_Zero: Toward Neurocognitive Foundations for Generative Social Science*. Princeton University Press.
11. Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research*, *72*(3), 199-200.
12. Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171-198.
13. Holt, T. J., Strumsky, D., Smirnova, O., and Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891-903.
14. Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60.
15. Jordan, T., and Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.
16. McKay, M. D., Beckman, R. J., & Conover, W. J. (1979). Comparison of three methods for selecting values of input variables in the analysis of output from a computer code. Technometrics, 21(2), 239-245.
17. Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. (2008). *The "big picture" of insider IT sabotage across US critical infrastructures* (pp. 17-52). Springer US.
18. Nagin, D. S., and Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law and Society Review*, 467-496.
19. Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers and Security*, *31*(4), 418-436.
20. Paternoster, R., and Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549-583.
21. Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3). MIT press.
22. Sokolowski, J., Banks, C., and Dover, T. (2016). An agent-based approach to modeling insider threat. *Computational and Mathematical Organization Theory*, 1-15.
23. Tibbetts, S. G., and Gibson, C. L. (2002). Individual propensities and rational decision-making: Recent findings and promising approaches. *Rational choice and criminal behavior: Recent research and future challenges*, 3-24.
24. Verizon. 2015 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2015/. Accessed on September 7, 2015.
25. Xu, Z., Hu, Q., and Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64-74.