A Behavioral Game Modeling Cyber Attackers, Defenders, and Users

Sarah Kusumastuti[1,2], Jinshu Cui[1,2], Arjun Tambe[1], and Richard S. John[1,2]
[1]Center for Risk and Economic Analysis of Terrorism Events (CREATE)
[2]Department of Psychology
University of Southern California
Los Angeles, CA
{kusumast,jinshucu,richardj}@usc.edu; arjuntambe@yahoo.com

Abstract

This paper describes a cyber-security game involving three players: attacker, defender, and user. This behavioral game is intended to capture key parameters that moderate the sequential multiplayer interaction among attackers, defenders, and users. Mini-max solutions for all three players are derived. We describe a behavioral experiment designed to validate model implications and identify game parameters that influence player behavior.

1. Introduction

With the vast and rapid integration of digital networks in many aspects of our lives comes more effort from criminals to target cyber networks, including cororate systems, social media, and government networks. Cyber attacks have developed from a simple effort to exploit a specific vulnerability to more wide reaching and persistent attacks towards interconnected networks.

Game theory is a paradigm that captures the interactions among members of a cyber landscape and frames the problem as a multiplayer adversarial game between attacker (cyber criminals), defenders (system security experts), and users (consumers or clients of the secure system).

Each player in the game has their own objectives and considerations in strategizing in the context of a particular cyber attack scenario. The choices each player makes must account not only their own potential rewards and penalties, but also potential rewards and penalties for other players. For instance, when a defender decides to employ security measures to protect the system from cyber-attacks, they must balance between maximizing system protection, maximizing user productivity, and minimizing costs..

Game theory is helpful in parsing the behavioral patterns that arise from the above scenario because it applies mathematical approaches in analyzing human strategizing and has been recently used in solving computer and communication networks (Anderson and Moore 2006). The application to cyber security scenarios is a matter of reframing the problem to reflect not only technological, but also psychosocial aspects of the interaction.

In this paper we develop a behavioral game to simulate a 3-player security game among attacker, defender, and user. The next section will describe the players, their roles and objectives. Section 3 describes an experimental design for studying security choices as a function of game parameters, and possible applications of the proposed game to specific cyber security contexts.

2. Cyber Security Game

This section describes a general cyber security game between attacker, defender, and user. We characterize the players' alternative space, rewards and penalties with a fully parameterized description of rewards and penalties.

2.1 Players

In our adversarial cyber security game the players are attackers, users, and defenders.

Attackers are entities that attempt to breach the security of their targets in order to obtain information. Attackers can be categorized according to many criteria. Among various types of attackers, the following entities present distinct threats: criminal, terrorist, foreign government, foreign military, non-state combatant, business and terrorist (Parker 1998). Attackers may choose to target large networks such as social media platforms or specific individuals.

Another dimension we put into account is the possibility of an attacker discovering a vulnerability in the system or gaining an exploitation technique that can massively increase their chances to successfully breaching the defender's security, but the nature of gaining these capabilities are stochastic. Consider an attacker seeking to identify a security bug in the system and to exploit that bug to attain their goal. An attacker can choose to immediately use that capability, or wait for a better time to use it with the risk that either the system administrator discovers and fixes that bug or another attacker discovers it and uses it to their advantage.

Defenders are security professionals who are in charge of protecting the computer system which is also partly responsible for user security. Defenders should consider the level of security they impose based on several factors, including both cost and user satisfaction. Higher security is often associated with higher cost and more restrictions for users of the system, which can lead to lower user satisfaction. Because of defenders' expertise and access to resources, it is much more difficult for an attacker to break into the defender's security, involving a high level of risk and typically requiring a large investment of time and effort, a relatively low chance of success, potential legal consequences, but very high potential rewards, related to attacker objectives, e.g., financial gains, obtaining sensitive information, signaling, etc. (Parker 1998)

Users are individuals connected to a system but who establish their personal security levels. There is substantial variance in how users apply their own security measures, accounting for aspects such as convenience or familiarity with cyber security protocols. However, in general, user security is expected to be much less sophisticated than the system security measures employed by the defender. It is typically easier to directly attack an individual user, but the reward is typically relatively fairly low, unless the target is a high profile user.

2.2 Decision Spaces for Three Players

For each game round, players choose an option and the outcome of the game is determined probabilistically. The decision space for each player in our game is as follows:

Attacker

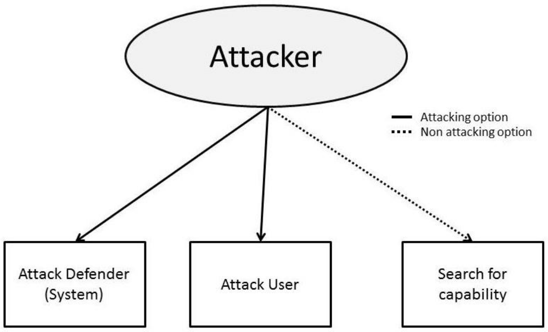

Figure 1: Attacker decision space

The attacker has the option to attack the different targets or to not attack and allocate effort to search for a capability that may boost their ability to attack the defender in future rounds. An attack towards the defender may have a large cost because they have more sophisticated security measures, although a successful attack offers a larger reward. A successful attack also provides the opportunity for the attacker to hurt the user, since without system protection a user becomes more vulnerable to security breaches.

The nature of discovering a capability is stochastic and involves a significant allocation of time and energy. Without capability, there is very little chance of success in attacking the system.

Directly attacking a user is another option for the attacker. Such an attack requires fewer resources to attack and a higher chance of success, but the reward is much less than a successful attack directed towards the system.

Defender

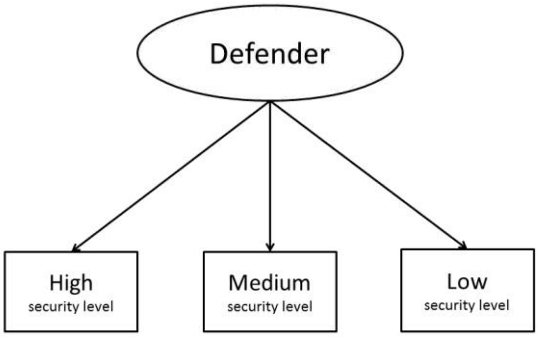

Figure 2: Defender decision space

The defender's decision space consists of the different level of security it can impose on the system. Higher level of security offers higher protection towards attacks, but is more onerous for users and costs more. A failure to defend from attacks depends on the defender's security level.

User

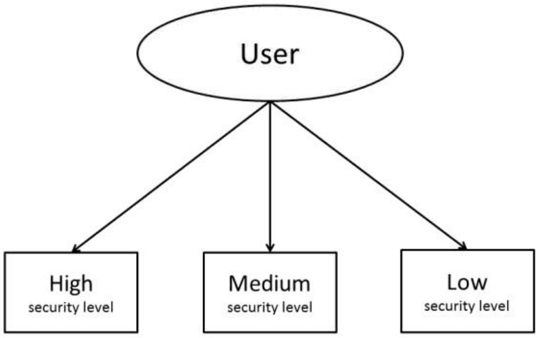

Figure 3: User decision space

The user decision space also consists of security level settings, but failure to defend from attacks towards the user depends both on the user and defender security settings. Another consequence of user's dependency on the defender includes potential losses when an attacker successfully attacks the system. Users are always vulnerable to cyber attacks, whether they are personally targeted or the system they are depending on is attacked.

To better characterize options for each player, we have generated equations describing rewards and penalties for each player which will be discussed in the next section.

2.3 Probabilities and Payoffs for Three Players

Attacker

Probability of Success

Attackers are in one of two states: without the capability to penetrate a system and with the capability to penetrate a system. We assume the capability is only related to the targeted system (defender). When an attacker has not obtained such a capability, the successful rate of compromising a system is extremely low. Therefore we say there are two options an attacker can choose from with no capability is to either invest to obtain a capability or attack users directly. When an attacker has obtained a capability, there are still two strategies: either attack the system using the capability or attack users.

With no capability to compromise the system, the probability of successfully obtaining a capability depends on the security level of the defender of the targeted system. The higher the defender's security level, the harder it is to break in the system, therefore the lower the probability of obtaining the capability. On the other hand, the probability of successfully attacking users depends on both defender's and users' security level. When the security level of users is low, it is easy for the attacker to obtain personal information; however, if the defender has forced the user to be in a high-security system, it is still hard for the attacker to break in. For instance, if the system that the user is using does a good job in blocking suspicious attempts from an attacker (e.g., gmail filter), the user is safe. Of course, the user can allow access to his/her account manually (e.g., open a spam email), which can also increase the attacker's likelihood of success.

After obtaining a capability to penetrate a system, the success rate of compromising a system becomes much higher than before. However, the success rate is still related to defender's system security level where it is harder to compromise the system when the defender imposes a high security level. Again, the probability of compromising a user depends on both defender's and users' chosen security levels, which is independent of the capability state of the attacker.

Cost, Reward and Penalty

The cost of obtaining capability is higher than attacking the system and the user because it involves investments in time, money and resources. The cost of attacking the user is lower than attacking the system because the time and effort spent in penetrating a system is greater.

The reward of compromising a system is much higher than compromising a user because the information obtained from a system contains all users' information in the system which could be many times that of a single user. On the other hand, the penalty is also higher if the system attack fails because the crime is bigger. Also it is more likely that the defender will find the attacker and make an appeal to him/her.

There is no instant reward or penalty for an attacker attempting to obtain the capability of compromising a system; however, an attacker expects to receive a reward in the future when the capability is obtained and information is successfully obtained from the targeted system.

Figure 4 (a) and (b) delineate the decision trees for attackers before and after capability is obtained.

Defender

Probability of Success

The probability of success for defenders is the probability that a defender is able to protect the system. Defenders can choose from three security levels: high, medium and low. Since the defender has no idea whether the attacker has obtained the capability, they need to consider both situations (West 2008).

When the attacker has not obtained a capability, the attacker can choose between obtaining the capability and attacking users. If the attacker chooses to invest in obtaining a capability, the system will always remain safe (probability of success is 1) in that particular round. If the attacker chooses to attack the user, the system is safe if the attacker fails but is vulnerable if the user's information is obtained because the attacker can further break into the system using user's information, although the probability is very small. Therefore, the probability of success for defenders if the attacker chooses to attack the user without capability depends largely on users' security level where the higher the user's security level, the higher the probability of keeping the system safe.

When the attacker has obtained a capability, the attacker can choose between attacking the defender or the user. The probability of success when the attacker chooses the user is the same as that when the attacker has no capability and chooses the user. If the attacker chooses to attack the system, the probability of success only depends on defender's own security level: higher with higher security level. Of course, it is harder to protect the system safe when the attacker targets the system than when the attacker targets the user.

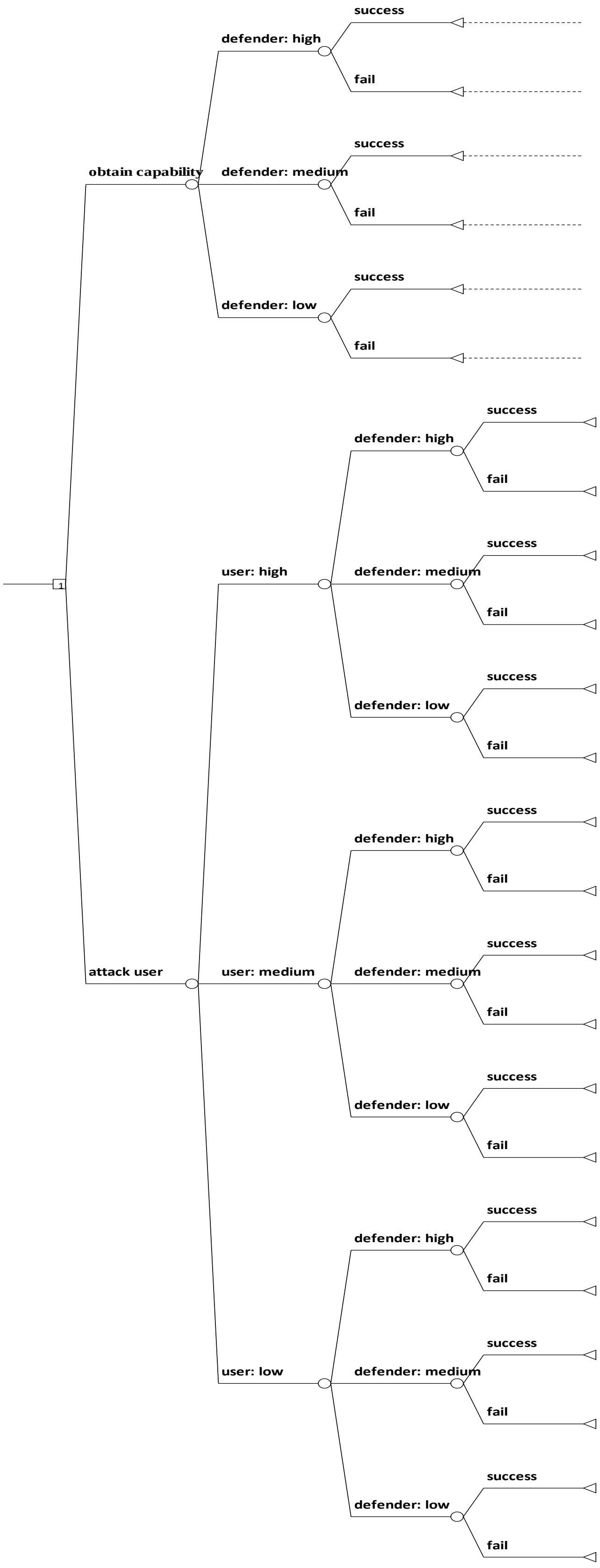

Figure 4 (a): Attacker decision tree without capability

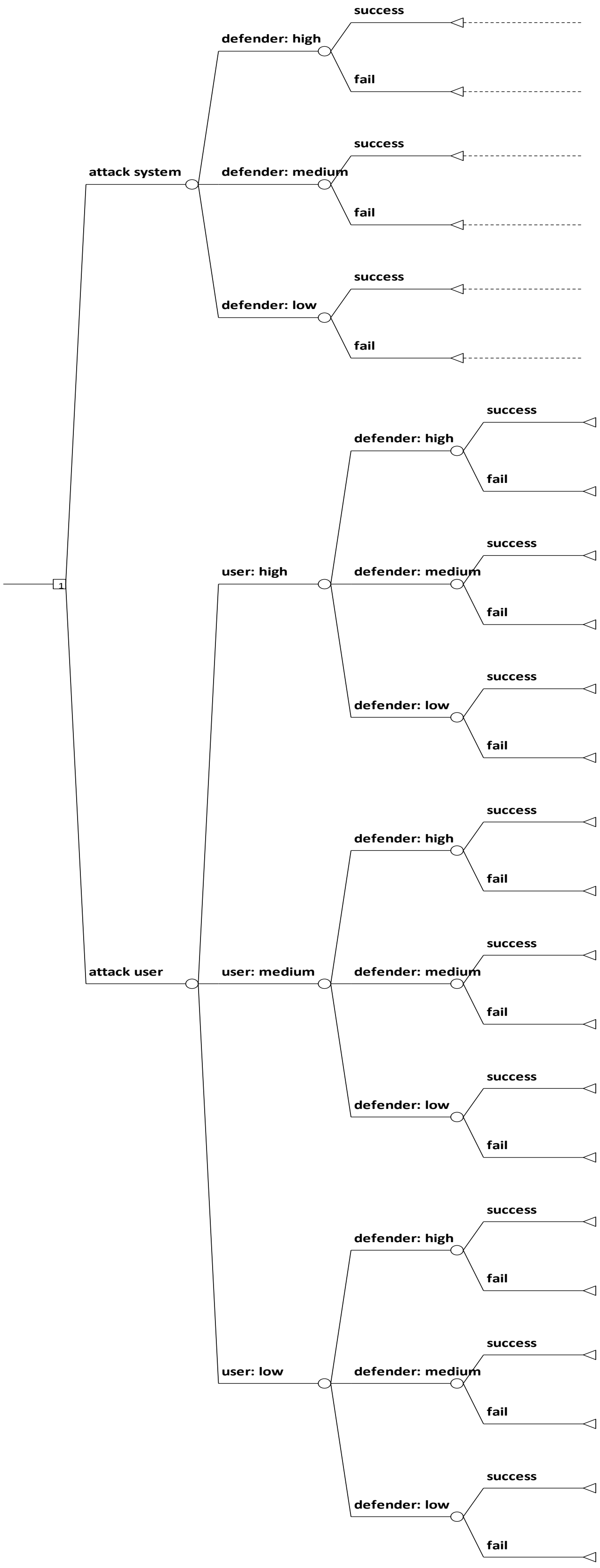

Figure 4 (b): Attacker decision tree with capability

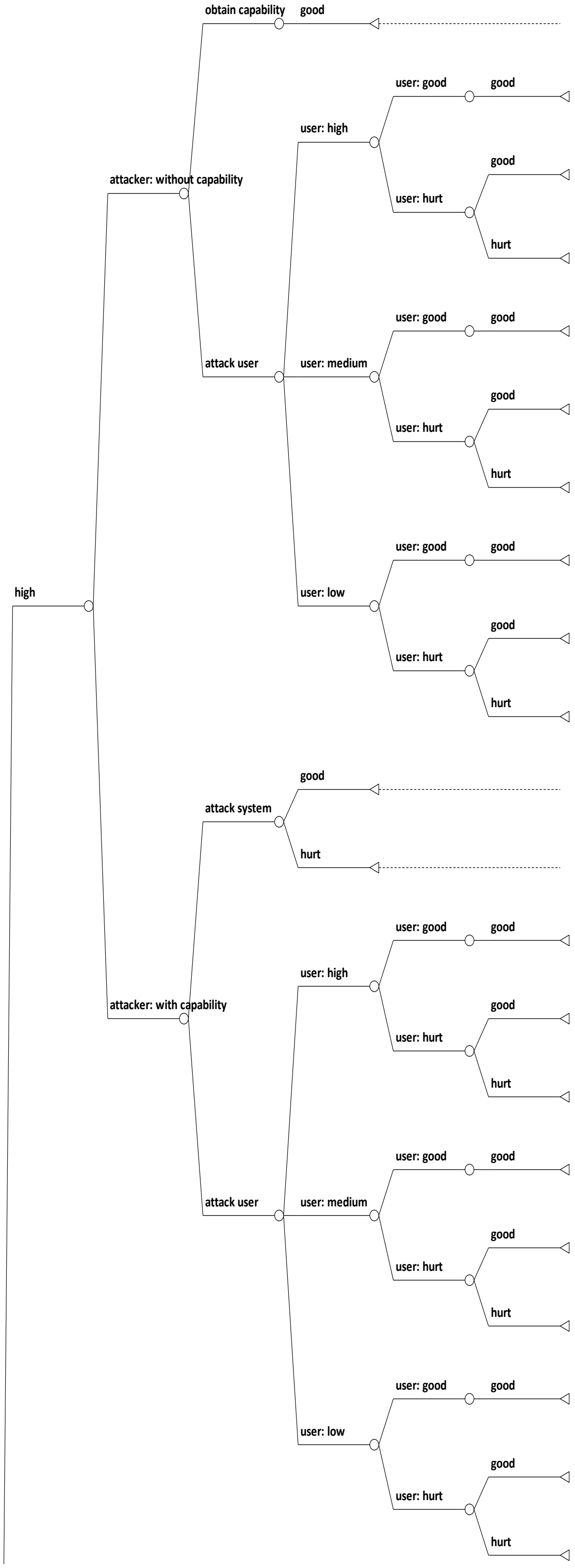

Figure 4 (c): Section of a Defender Decision Tree

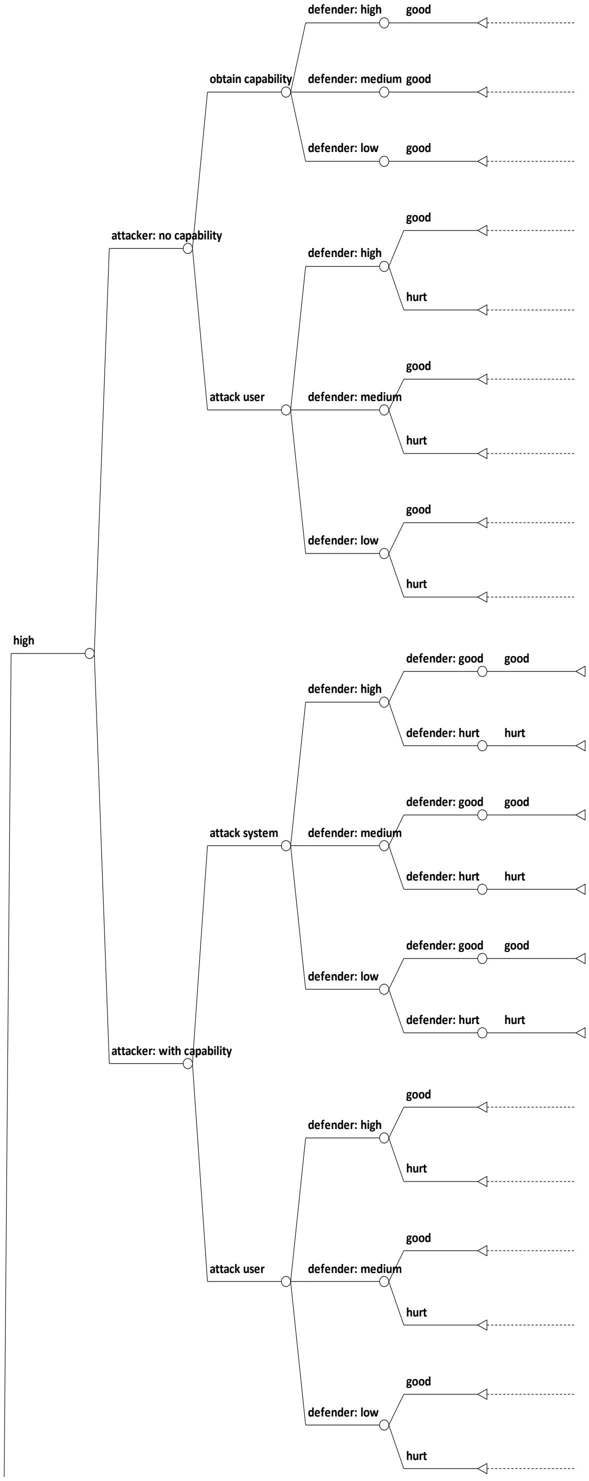

Figure 4 (d): Section of a User Decision Tree

Cost, Reward and Penalty

The cost of defenders is high for high security level. Besides the investment on keeping the system safe, the defender can also lose users because the high security level of the system will lower the convenience and productivity of the user.

The reward and penalty for defenders does not vary. The defender receives a reward when the system is safe and receives a penalty when the system is compromised.

The subtree for defenders selecting a high security level is depicted in Figure 4 (c) (subtrees for medium and low level are the same with high level and the whole decision tree consists the three subtrees).

User

Probability of Success

The probability of success for users means the probability that a user's information is not obtained by an attacker. Like defenders, users can choose among three security levels: high, medium and low. Users may consider whether the attacker has obtained the capability to attack the system.

When the attacker has not obtained the capability and chooses to obtain a capability, the probability of success for users is always 1. If the attacker chooses to attack the user, the higher security level is set by the user, the less likely the attacker can obtain the user's personal information. The probability of success also depends on defender's security level because the user will more likely to be safe if he/she is using a well-protected system. For example, some browsers are safer than others in terms of blocking the access to suspicious websites.

When the attacker has obtained the capability and chooses to attack the user, the probability of escaping the attack is again the same with that when the attacker has no capability and chooses to attack the user. If the attacker chooses to attack the system, the probability of success is determined by defender's security level. If the system is compromised, the user whose information is in the system will also be compromised; whereas if the system is safe, the users' information is also safe. Therefore, the higher the system's security level is, the high the probability of success for the users.

Cost, Reward, and Penalty

Again, higher security level means higher cost. For example, a user needs more time and/or more money to purchase a desired video if she refuses to download it from a suspicious link.

The penalty of losing personal information does not vary with the three player's choices. However, the reward of avoiding the leak of personal information is related to the defender's security level. When the system's security level is high, the convenience level and productivity of the user will decrease. For instance, the user needs to click "allow access" every time a window pops up asking for system access to install a new application or update. Also, the user may have no access to some websites even though they are safe.

Figure 4 (d) delineates the subtree for users with high security level (subtrees for medium and low level are the same with high level and the whole decision tree is formed by the three subtrees).

2.4 Optimal Strategies solved by Minimax

The minimax equations for all three roles represent the choice that minimizes loss given a worst case scenario. This equation can be translated to the game in the form of probabilities for success in attacking the intended target.

The parameters of the equation represent the independent variables that can be varied to test the model. Because of the adversarial nature of the game, the optimal strategy for each player depends on the decisions of other players. In this case, the parameters include the base cost of the options, along with the costs of the worst case option. The number of parameters is determined by the number of terms in the equation.

For the following equations, some abbreviations we will be using are *atk* for attacker, *df* for defender, and *u* for user, *h* for high security, *m* for medium security, and *l* for low security level.

Attacker

For the attacker, there will be four cases describing options because the valuation of attacking the defender will be affected by attacker capability state. A success in the defender's case is a success in penetrating the security system of the defender, user, or both.

1. Attack Defender without capability

   $\max(cost) = cost(df(h)) + cost(attack(df))$
   $= p(success\colon df(\ h)) \times reward + \ p(fail\colon df(h))$
   $\times penalty + \ cost(attack(df))$

2. Attack Defender with capability

   $\max(cost) =$
   $cost(df(h), capability(yes)) + cost(attack(df)) =$
   $p(success\colon df(h), capability(yes)) \times reward\ +$
   $p(fail\colon df(h), capability(yes)) \times penalty +$
   $cost(attack\ (df))$

3. Attack User

   $\max(cost) = cost(df(h), u(h)) + cost(attack(u))$
   $= p(success\colon df(h), u(h)) \times reward$
   $+\ p(fail\colon df(h), user(h)) \times penalty$
   $+\ cost(attack(u))$

4. Search for capability

   $cost(obtain\ capability) = c(o)$

Therefore, in the state of having capability, the optimal choice would be the minimum among equations 2, 3, and 4. For the situation where the attacker does not have a capability, equation 1 is used instead, so the option will be the minimum among equations 1, 3, and 4.

For the attacker, there are a total of 9 parameters included in the equations above that can be manipulated. Note that the base cost of attacking the defender is the same whether the attacker has a capability or not

Defender
The defender's equations depend on the security setting. The probability of success for the defender is the probability that the defender successfully protects the system from a cyber attack. The worst case scenario for the defender will always have the attacker attacking with capability

1. High security setting
   $\max(cost) = cost(h) + cost(capability(yes), df(h))$
   $= cost(h) + p(success: capability(yes), df(h))$
   $\times reward + p(failure: capability(yes), df(h))$
   $\times penalty$
2. Medium security setting
   $\max(cost)$
   $= cost(m) + cost(capability(yes), df(m))$
   $= cost(m) + p(success: capability(yes), df(m))$
   $\times reward + p(failure: capability(yes), df(m))$
   $\times penalty$
3. Low security setting
   $\max(cost) = cost(l) + cost(capability(yes), df(l))$
   $= cost(l) + p(success: capability(yes), df(l))$
   $\times reward + p(failure: capability(yes), df(l))$
   $\times penalty$

Therefore, the optimal choice would be the one that minimizes the costs of all three options. There are 9 parameters from the equations above.

User
The users' dependency on the defender results in some further dependencies in the equations. The first dependency is that a successful attack on the user does not only depend on the user's security level but also the defender's. Another dependency is that the user also possess a risk of penalty in the event of a successful attack on the system. This results in the user equations having parameters that are dependent on the defender's choice, but for the worst case scenario, we always assume that the defender has the lowest security. Similar to the defender, success for the user means that the user successfully defends from attack

1. High security setting
   $\max(cost)$
   $= cost(h) + \max(cost(h, attack(df), df(l)),$
   $cost(h, attack(u), df(l))$
   $= cost(h) + \max(p\big(success: attack(df), df(l)\big)$
   $\times reward + p\big(fail: attack(df), df(l)\big)$
   $\times penalty, p(success: h, attack(u), df(l)) \times reward$
   $+ p\big(fail: u, attack(u), df(l)\big) \times penalty)$
2. Medium security setting
   $\max(cost)$
   $= cost(m) + \max(cost(m, attack(df), df(l)),$
   $cost(m, attack(u), df(l))$
   $= cost(m) + \max(p(success: attack(df), df(l))$
   $\times reward + p(fail: attack(df), df(l))$
   $\times penalty, p(success: m, attack(u), df(l)) \times reward$
   $+ p(fail: m, attack(u), df(l)) \times penalty)$
3. Low security setting
   $\max(cost)$
   $= cost(l) + \max(cost(l, attack(df), df(l)),$
   $cost(l, attack(u), df(l))$
   $= cost(l) + \max(p(success: attack(df), df(l))$
   $\times penalty + p(fail: attack(df), df(l))$
   $\times reward, p(success: l, attack(u), df(l)) \times reward$
   $+ p(fail: l, attack(u), df(l)) \times penalty)$

For the optimal choice, the user should choose the option that has the minimal cost between all three security settings. There are 11 parameters involved in the user minimax equations.

It is possible that no pure strategy exists. For example, when the attacker has obtained the capability, usually the best choice is to use it to attack the system. However, this may not always be the optimal strategy. When the system's security level is high, the probability of compromising the system could be similar to the probability of compromising a user; given the high cost of attacking a system, the optimal strategy when system's security level is high could be attacking the users. While it is more profitable to attack the system when security level is medium or low, a mixed strategy with a high probability of attacking the system and a low probability of attacking the users should be considered.

3. Future Developments

The data obtained from the behavioral experiment will consist of the choices made by each player throughout the game as well as the allocation of resources that is made throughout the game. This information helps to model the strategy that is used by the subjects and to assess the extent to which they follow the minimax algorithms or whether they fit other decision models.

The independent variables can also be varied to investigate whether subjects are sensitive to the change of certain parameter values such as cost, reward, or probability of success and change their strategy.

The data obtained from this experiment will be used to construct bots that simulate certain strategy models employed by the players. The ability to create such bots is useful to test various specific hypotheses about player choices. With bots, it is easier to simulate more realistic cyber security networks with thousands of users.

The next step includes developing the game for different cyber contexts and adjusting dependencies so that the game is a realistic representation of important cyber security domains.

For example, a game with multiple users that are connected to one system can be developed into a game where there are high profile and low profile users and attacks to certain users provides a high reward. This affects the attacker's target valuation as there is now multiple targets with various levels of importance and difficulty.

From the defender's paradigm, we can set the game so that the defender has to take into account the users' level of satisfaction with the security system. Tighter security measures often require more restrictions for users, which may cause dissatisfaction (Kabay 2009). This adds another constraint to the defender because they would not only be balancing cost and security, but also the level of user satisfaction.

An example of the extension of a game that involves the attacker is giving the choice of saving their capability to be used at a more strategic time, or to construct the capability as a continuum and create the possibility of having multiple capabilities. This feature will also be beneficial in creating a game with multiple attackers that are competing with each other.

The context of the cyber security game itself can be adapted to more specific scenarios such as an attack on financial institutions such as banks or credit card companies, attacks on online file storage, password security, and even government Information Technology (IT) systems. Furthermore, the development of behavioral experiments to test game theoretic models in cyber security is essential to incorporating human behavior in cyber security.

Acknowledgements

This research was supported by the National Science Foundation under grant number SES-1314644. It was also supported by the U. S. Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events under the cooperative agreement number 2010-ST-061-RE0001. However, any opinions, findings, conclusions, and recommendations in this document are those of the author and do not necessarily reflect views of the National Science Foundation or the U. S. Department of Homeland Security. We would like to thank Heather Rosoff, Detlof von Winterfeldt, Michael Orosz, Jim Blythe and Tanya Ryutov for their support.

References

Anderson, R., and Moore, A. 2006. The Economics of Information Security. *Science* 314:610-613.

Aytes, K., and Conolly, T. 2003. A Research Model for Investigating Human Behavior related to Computer Security. In Proceedings of the 9th Americas Conference on Information Systems, 260. Tampa, Florida. Association for Information Systems

Aytes, K., and Connolly, T. 2005. Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Advanced Topics In End User Computing* 4:257.

Funderberg, D., and Tirole, J. 1992. *Game Theory*. Cambridge, Mass.: MIT Press.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., and Byrne, Z. 2012. The Psychology of Security for the Home Computer User. In *Security and Privacy (SP), 2012 IEEE Symposium on*, 209-223. San Francisco, Calif,: IEEE.

Kabay, M. E. 2009. *Computer Security Handbook, 5th Edition*. New York: John Wiley & Sons Inc.

Lesk, M. 2011. Cybersecurity and Economics. *Security & Privacy, IEEE* 9(6): 76-79.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 45(3), 25.

Parker, D. B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, Inc..

Shaw, E., Ruby, K., and Post, J. 1998. The Insider Threat to Information Systems: The Psychology of the Dangerous Insider. *Security Awareness Bulletin* 2(98): 1-10.

Uma, M., and Padmavathi, G. 2013. A Survey on Various Cyber Attacks and their Classification. *IJ Network Security* 15(5), 390-396.

Wang, S., and Ledley, R. S. 2012. *Computer Architecture and Security: Fundamentals of Designing Secure Computer Systems*. New York: John Wiley & Sons.

West, R. 2008. The Psychology of Security. *Communications of the ACM* 51(4): 34-40.