

DEFINING ATTACKER BEHAVIOR PATTERNS IN THE CONTEXT OF  
AN INFORMATION SYSTEM

A Dissertation

Presented in Partial Fulfillment of the Requirements for the  
Degree of Doctor of Philosophy

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

by

Mark Rounds

May 2014

Major Professors

Jim Alves-Foss Ph.D.

Norman Pendegraft Ph.D.

### Authorization to Submit Dissertation

This dissertation by Mark Rounds submitted for the degree of Doctor of Philosophy with a major in Computer Science and titled “DEFINING ATTACKER BEHAVIOR PATTERNS IN THE CONTEXT OF AN INFORMATION SYSTEM” has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor \_\_\_\_\_ Date \_\_\_\_\_  
James Alves-Foss

Major Professor \_\_\_\_\_ Date \_\_\_\_\_  
Norman Pendegraft

Committee  
Members \_\_\_\_\_ Date \_\_\_\_\_  
Paul Oman

\_\_\_\_\_ Date \_\_\_\_\_  
Terence Soule

\_\_\_\_\_ Date \_\_\_\_\_  
Bob Stone

Computer Science  
Administrator \_\_\_\_\_ Date \_\_\_\_\_  
Gregory Donohoe

Engineering  
College Dean \_\_\_\_\_ Date \_\_\_\_\_  
Larry Stauffer

Final Approval and Acceptance by the College of Graduate Studies

\_\_\_\_\_ Date \_\_\_\_\_  
Jie Chen

## **Abstract**

Information systems are pervasive in our everyday life. Anyone who is online must deal with the consequences of the fact that such systems are prone to malicious attack. In our attempt to safeguard our systems, determination of the value of security measures is critical and is an area currently undergoing scrutiny by many researchers. There has been much research and development done on various technological security tools but there has been less work on the human side of computer security. One method to determine the actions and the intent of attackers in this environment is to simulate interactions between an information system, its users, and a population of attackers. Initial simulation results suggest that the marginal value of additional security may be positive or negative, as may the time rate of change of system value. Models created with this in mind have shown some predictive value, but are based on certain strong assumptions. In particular, our model assumes that the attacker's response to changes in a system's value and security are "S" shaped. The goals of this dissertation are to support or refute these assumptions to make a more predictive model. Results of this work supports the hypothesis that these curves are in fact "S" shaped.

## **Acknowledgements**

I would like to acknowledge my advisors, Norman Pendegraft and Jim Alves-Foss for their support and persistence through this process. I would like to acknowledge Elliot Rich of the University of Albany for making clear to me the reasoning behind “S” shaped curves in dynamic modeling at HICSS 46. I would like to acknowledge Thia Kaag who has been my copy editor. The College of Business and Economics was also supportive of this work through a summer research grant. Charlie Bales was also helpful in developing the first revision of the testing software.

### **Dedication**

I would like to thank my wife, Susan, and children, Jani, Garret, and Bethany, for putting up with me and supporting me through this process. I would also like to thank Professor Bitterwolf in the Chemistry Department as he, along with Don Kaag, convinced me that it was a good idea to continue my education. My parents are no longer with us but I am still very grateful that they encouraged and supported their child who the school system thought was backward. They earned this every bit as much as I did.

## Table of Contents

<b>Authorization to Submit Dissertation .....</b>	<b>ii</b>
<b>Abstract.....</b>	<b>iii</b>
<b>Acknowledgements.....</b>	<b>iv</b>
<b>Dedication .....</b>	<b>v</b>
<b>Table of Contents .....</b>	<b>vi</b>
<b>List of Figures.....</b>	<b>ix</b>
<b>List of Tables .....</b>	<b>xii</b>
<b>Chapter 1. Background .....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Background.....	1
1.2.1 Human Factors .....	1
1.2.2 The Curve.....	3
1.2.3 Users .....	5
1.2.4 Honeypots .....	6
1.2.5 Utility .....	6
1.3 Hacker Demographics .....	7
1.3.1 How do you categorize attackers?.....	7
1.3.2 Hackers.....	8
1.3.3 Hacker Demographics.....	10
1.3.3.1 Script Kiddies.....	10
1.3.3.2 Malware Developers .....	11
1.3.3.3 Hactivists.....	12
1.3.3.4 Vigilantes .....	13
1.3.3.5 State Sponsored Hacking .....	13
1.3.3.6 Professional Criminal.....	14
1.3.4 Hacker Life Cycle .....	15
1.3.5 Hacker Longevity.....	15
1.3.6 Hacker Groups .....	16
1.3.7 Basic Approach .....	17
1.4 Research Question .....	17
1.4.1 First Hypothesis .....	17
1.4.2 Second Hypothesis .....	18

<b>Chapter 2. General Simulation Model .....</b>	<b>19</b>
2.1 Computer Security Problem .....	19
2.2 Methodology / Simulation Background.....	20
2.3 The Model.....	22
2.3.1 Conceptual Background .....	22
2.3.2 IThink Model .....	27
2.4 Discussion of Model Results .....	30
<b>Chapter 3. Experimental Methodology.....</b>	<b>40</b>
3.1 Research Direction.....	40
3.2 Experimental Design Background.....	40
3.3 Validation of Methodology.....	41
3.4 Methodology Background .....	42
3.5 Initial Steps .....	44
3.6 Experiment 1.....	45
3.7 Experiment 2.....	49
3.8 Experiment 3.....	50
3.9 Software Framework .....	50
3.9.1 Consent Screen.....	51
3.9.2 Demographics Screen.....	52
3.9.3 Computer Self Efficacy Quiz Screen .....	53
3.9.4 The Test.....	54
<b>Chapter 4. Results .....</b>	<b>56</b>
4.1 Analysis of Observations .....	56
4.1.1 Research Question.....	56
4.1.2 Hypothesis.....	56
4.1.3 Analysis of Experiment 1 .....	58
4.1.4 Clustering .....	64
4.1.5 The Top Cluster.....	66
4.1.6 The Bottom Cluster .....	69
4.2 Analysis of Experiment 2 .....	72
4.2.1 Hypothesis for Experiment 2.....	72
4.2.2 Analysis for Experiment 2 .....	74
4.2.3 Graphical Analysis for Experiment 2.....	75

4.2.4 Graphical Analysis for Experiment 2 Top Cluster .....	79
4.2.5 Graphical Analysis for Experiment 2 Center Cluster.....	81
4.2.6 Graphical Analysis for Experiment 2 Bottom Cluster .....	83
4.3 Analysis of Experiment 3 .....	86
4.3.1 Hypothesis for Experiment 3.....	86
4.3.2 Graphical Analysis for Experiment 3.....	87
4.3.2 Graphical Analysis for Experiment 3 Top Cluster .....	91
4.3.3 Graphical Analysis for Experiment 3 Center Cluster.....	93
4.3.4 Graphical Analysis for Experiment 3 Bottom Cluster .....	96
4.3.5 Graphical Analysis for Experiment 3 Fraternity Cluster.....	98
4.3.6 Computer Efficacy .....	101
<b>Chapter 5. Discussion and Conclusion .....</b>	<b>102</b>
5.1 Discussion.....	102
5.2 Lessons Learned .....	104
5.3 Conclusions.....	106
5.4 Future Work.....	106
<b>Chapter 6. References.....</b>	<b>109</b>
<b>Appendix I Computer Self Efficacy Quiz .....</b>	<b>119</b>
<b>Appendix II IRB Approval.....</b>	<b>122</b>



## List of Figures

Figure 1. Attack vs. Security.....	4
Figure 2. Basic Model .....	24
Figure 3. Value vs. Use and Attacks .....	26
Figure 4. Attacks vs. Security .....	26
Figure 5. Ithink Model .....	28
Figure 6. Model Equations .....	29
Figure 7. $S_u^*$ is Large, (+,-)Value is Increasing, Security is Detracting from Value .....	31
Figure 8. $S_a^*$ is Large, (+,+) Value is Increasing, Security is Enhancing Value .....	32
Figure 9. $S_a^*$ is Large (-,-) Value is Decreasing, Security is Detracting from Value .....	32
Figure 10. $S_u^*$ is Small (-,+)Value Decreasing but Additional Security Lessens Decrease .....	33
Figure 11. Response Graph .....	33
Figure 12. Response is Concave .....	35
Figure 13. Reponse is Convex .....	35
Figure 14. Response (0,0) Value and Security Remain Unchanged .....	36
Figure 15. Response (+,0) Value Increases but is not Effectted by Security .....	36
Figure 16. Response (-,0) Value Decreases but is not Effectted by Security .....	37
Figure 17. Consent Screen .....	51
Figure 18. Demographics Screen .....	52
Figure 19. Computer Efficacy Quiz .....	53
Figure 20. The Experiment .....	54
Figure 21. Experiment 1, Total Number of Attempts vs. Number of Passwords Possible.....	60
Figure 22. Experiment 1, Number of Attempts vs. Number of Passwords Possible.....	61
Figure 23. Experiment 1, Number of Participants at Each Level vs. Number of Passwords Possible .....	62
Figure 24. Experiment 1, Number of Successes at Each Level vs. Number of Passwords Possible .....	62
Figure 25. Experiment 1, Number of Attempts vs. Number of Passwords Possible with Cluster Circled.....	64
Figure 26. What Cluster Analysis Captures .....	65

Figure 27. Experiment 1, Number of Attempts vs. Number of Passwords Possible for the Top Cluster .....66

Figure 28. Experiment 1, Number of Attempts vs. the Number of Passwords Possible for the Top Cluster for the Last Four Data Points.....67

Figure 29. Experiment 1, Number of Participants vs. Number of Passwords Possible at Each Level for the Top Cluster .....68

Figure 30. Experiment 1, Number of Successes vs. the Number of Passwords Possible at Each Level for the Top Cluster .....68

Figure 31. Experiment 1, Number of Attempts vs. Number of Passwords Possible at Each Level for the Bottom Cluster .....70

Figure 32 Experiment 1, Number of Participants vs. Number of Passwords Possible at Each Level for the Bottom Cluster .....70

Figure 33. Experiment 1, Successes vs. Number of Passwords Possible at Each Level for the Bottom Cluster .....71

Figure 34. Experiment 2, Number of Attempts vs. Reward Level for the Whole Population.....75

Figure 35. Experiment 2, Number of Attempts vs. Reward Level for the Whole Population Clusters Circled.....76

Figure 36. Experiment 2, Number of Participants vs. Reward Level for the Whole Population .....76

Figure 37. Experiment 2, Number of Successes vs. Reward Level for the Whole Population .....77

Figure 38. Experiment 2, Number of Participants vs. Reward level Possible with Clusters Circled .....78

Figure 39. Experiment 2, Number of Attempts vs. Reward Level for the Top Cluster.....79

Figure 40. Experiment 2, Number of Participants vs. Reward Level for the Top Cluster .....80

Figure 41. Experiment 2, Number of Successes vs. Reward Level for the Top Cluster .....80

Figure 42. Experiment 2, Number of Attempts vs. Reward Level for the Center Cluster .....82

Figure 43. Experiment 2, Number of Participants vs. Reward Level for the Center Cluster .....82

Figure 44. Experiment 2, Number of Successes vs. Reward Level for the Center Cluster .....83

Figure 45. Experiment 2, Number of Attempts vs. Reward Level for the Bottom Cluster .....84

Figure 46. Experiment 2, Number of Participants vs. Reward Level for the Bottom Cluster .....84

Figure 47. Experiment 2, Number of Successes vs. Reward Level for the Bottom Cluster.....85

Figure 48. Experiment 3, Number of Attempts vs. Reward Level for the Whole Population.....88

Figure 49. Experiment 3, Number of Participants vs. Reward Level for the Whole Population .....88

Figure 50. Experiment 3, Number of Successes vs. Reward Level for the Whole Population .....89

Figure 51. Experiment 3, Number of Participants vs. Reward Level Possible with Clusters Circled.....	90
Figure 52. Experiment 3, Number of Attempts vs. Reward Level for the Top Cluster.....	91
Figure 53. Experiment 3, Number of Participants vs. Reward Level for the Top Cluster .....	92
Figure 54. Experiment 3, Number of Successes vs. Reward Level for the Top Cluster .....	92
Figure 55. Experiment 3, Number of Attempts vs. Reward Level for the Center Cluster .....	94
Figure 56. Experiment 2, Number of Participants vs. Reward Level for the Center Cluster .....	94
Figure 57. Experiment 3, Number of Successes vs. Reward Level for the Center Cluster .....	95
Figure 58. Experiment 3, Number of Attempts vs. Reward Level for the Bottom Cluster .....	96
Figure 59. Experiment 3, Number of Participants vs. Reward Level for the Bottom Cluster .....	97
Figure 60. Experiment 3, Number of Successes vs. Reward Level for the Bottom Cluster.....	97
Figure 61. Experiment 3, Number of Attempts vs. Reward Level for the Fraternity Cluster .....	99
Figure 62. Experiment 3, Number of Participants vs. Reward Level for the Fraternity Cluster .....	99
Figure 63. Experiment 3, Number of Successes vs. Reward Level for the Fraternity Cluster .....	100

## List of Tables

Table 1. Initial Payment Rates .....	48
Table 2. Experiment 1, Complete Data Set .....	63
Table 3. Experiment 1, Top Cluster .....	69
Table 4. Experiment 1, Bottom Cluster.....	72
Table 5. Experiment 2, All Participants .....	78
Table 6. Experiment 2, Top Cluster .....	81
Table 7. Experiment 2, Center Cluster.....	83
Table 8. Experiment 2, Bottom Cluster.....	85
Table 9. Experiment 3, All Participants.....	90
Table 10. Experiment 3, Top Cluster .....	93
Table 11. Experiment 3, Center Cluster.....	95
Table 12. Experiment 3, Bottom Cluster.....	98
Table 13. Experiment 3, Fraternity Cluster.....	100
Table 14. Efficacy Scores for All Experiments.....	101
Table 15. Experiment 3, Cluster Attempts Comparison .....	105

## **Chapter 1. Background**

### **1.1 Introduction**

In Pendegraft, Rounds, and Frincke (2005) a dynamic model was developed to help predict the effect of changes in value and security in an information system. This model will be described in more detail later in this dissertation. The strongest assumption made is that the curves generated when comparing attacker behavior to changing information system value are “S” shaped. This means that the initial portion of the curve shows small marginal changes. As the independent variable increases or decreases, the slope steepens as the marginal change becomes significant. Then at the end, marginal change again becomes insignificant. While some work has been done on the shape of the curve for users (Pendegraft, in press), there is little work done regarding the attackers. The goal in this dissertation is to determine what attacker response curves look like.

### **1.2 Background**

Much of the research in the field of computer security focuses on technological systems interactions (Walters, Liang, Shi, and Chaudhary 2006). Significant portions of that work focuses on the technological problem of securing a wireless network, even though they state in the beginning that humans drive the bulk of the threats.

#### **1.2.1 Human Factors**

Another major focus of the literature concerning computer and network security focuses on the defender’s actions to protect his/her information system (Stallings 2006). This is partially because he/she is willing to be analyzed in the hope of making his/her job easier. Even when one is trying to search the literature for papers on “computer or network attackers,” a common experience has been that Google Scholar and other search engines try

to correct the keyword search to “computer attacks.” The focus is clearly on the attacks and the methodology, not the attacker and his/her motivations.

Udo’s survey (Udo 2001) of privacy and security concerns as related to e-commerce focuses on how users perceive threats. He concludes that while many information technology users feel that security is critical, they don’t believe that the government or any technological fix is capable of securing their privacy. The focus on the technology of security and the desire for a technological fix goes back to the early research surveyed by Brown (1976), which states that there were thousands of papers on computer security and risk management, most of which were too narrow in scope and too focused on technological fixes to be of much value.

Even in those papers where the information system/human interaction factor is described, the literature tends to focus on the technology rather than human factors. In their book, Cranor and Garfinkel (2005) make the excellent point that overly complex passwords can hurt the overall effectiveness of password security but instead of addressing this problem, the authors switch to a discussion of the technical details of passwords. While Besar and Arief (2004) and Duggan, Johnson, and Grawemeyer (2012) discuss the impairment of security by legitimate users, their description of the faults again focuses on the technical.

Sasse (Sasse, et. al. 2001) says that the human portion of the security problem is the area of highest leverage. Adams and Sasse (1999) state that rather than avoiding investigating the human factors, they need to be embraced. Describing the human factor interaction is critical because so many threats use humans in the system as a vector into the system (Mitnick and Simon 2002).

The human factor is important because engineers cannot evaluate a security system until they can measure the effectiveness and, hence, the benefit provided by computer security. Carayon (2006) describes the concept of a “sociotechnical system” which is the amalgamation of humans and their information systems. However, this description does not provide a measurement of security.

Saltzer and Schroeder (1975), recognize that humans play a role, but focus on technological issues of security rather than interactions of a system with users and attackers.

Many firms engage in cost/benefit analysis of security measures before imposing these measures (Gordon et.al. 2006, Farahmand, et.al. 2005). These analyses are primarily qualitative in nature since there are few quantitative models of the interaction between attacker and security professional. Previous work (Pendegraft, Rounds, and Frincke (2005); Pendegraft and Rounds (2006, 2007); and Rounds, Pendegraft, and Taylor (2007)) has generated some interesting conclusions on modeling the attacker/user relationship as it pertains to the value of an information system.

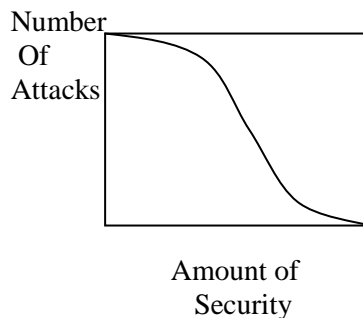
Pendegraft, Rounds, and Frincke (2005), and Pendegraft and Rounds (2006, 2007) suggest that when securing an information system, there are combinations of system value, security investment, user motivation, and attacker motivation where adding more security is detrimental to the system’s value. Results further suggest that under some circumstances changing these variables by educating the users or increasing effective enforcement as examples is a better use of resources than technological security measures.

### **1.2.2 The Curve**

During the initial stages of developing this methodology, data for random curves were generated, averages and graphed. These test results indicate that perhaps a straight line

is the best representation of attacker behavior, except that real world anecdotes do not support this hypothesis. For example, recently Russia attacked Georgia (Thomas 2009), preceding the physical attack with an intense cyber-attack. Clearly this was a dedicated group of attackers who had a very specific view of system value, a definite time limit, were highly skilled, and had considerable resources to draw upon (Stringer 2008). Their motivations were the same since they worked for the same agency. This suggests that they would have a similar response with regards to their response to security, a curve similar to other groups with similar motivations.

### Response to Increased Security



**Figure 1. Number of Attacks vs. Level of Security**

Modeling of attacker and user response to increasing security in Pendegraft, Rounds, and Frincke (2005), and Pendegraft and Rounds (2006, 2007) is based on several strong assumptions. One of the strongest assumptions is that the attacker's response to changing security and changing system value is an "S" shaped curve ( Figure 1). This curve is generated when the attack rate is compared to the level of security. In most populations, it means that at some point, the bulk of the attackers will not find this an acceptable target to



attack and if the attackers' motivations are similar, it tends to happen at about the same security level, hence the sharp drop off in the "S" shaped curve.

Yamada, Ouba, and Osaki (1983) indicate that curves focusing on error detection and response tend to be "S" shaped in this manner. Their methodology for measuring errors and intrusions is very similar to that in the papers cited above and supports the choice of an "S" shaped curve.

The graph in Figure 1 illustrates that at low levels of security, the number of attempts to compromise the system is high, because the level of effort required to gain the reward is low compared to the size of the reward. The number of attackers will decrease as the level of security increases because, as the level of effort increases, fewer attackers are willing to attempt compromising the system. Further, there is a point on the curve where the slope will decrease, then as the end of the range is reached and only a few stubborn attackers remain, the curve will flatten out. This is the basic assumption that generates the "S" shaped curve.

### **1.2.3 Users**

The main assumption following Becker's (1968) work with non-computer crime is that attackers in the on-line arena are motivated by economic goals and respond to the size of the reward and the ease at which that reward can be obtained. Riva (2004) says that there is a large population of individuals engaged in "for profit" attacks on information systems who are rational criminals. This is of value since any action with a rational basis more easily interpreted mathematically.

Gordon and Loeb (2002) describe how an information system manager might respond in terms of monetary resources for a selected vulnerability, but they do not discuss how this response will affect the likelihood of future attacks. Authors such as Schneier

(2004) and Cavusoglu, Cavusoglu, and Raghunathan (2004) look at the economics of computer security from the user's point of view but cast little light on how the attacker responds. Their work assumes that attackers are uniform in nature and focuses on the most cost effective combination of technological security measures.

Cavusoglu, Mishra, and Raghunathan (2004) have done some interesting work on a model that looks at a form of user utility, but the model focuses on reducing risk, not increasing the value of the information system they are trying to protect. Anderson and Moore's (2006) work on how to measure security argues that until you can measure security, you can't manage the risk it is supposed to minimize.

Cardenas et. al. (2012) discusses the consequences of security breaches for publicly traded companies as it relates to their stock price and valuation. Increased attacks seem to have a direct negative effect on the stock price.

#### **1.2.4 Honeypots**

There is a significant body of literature on the "Honey Pot" that presents a false website or other asset designed to attract attacks for the purpose of research or to deflect them from valuable assets (Spitzner 2003). "Honey Net" technology (Spitzner 2001) employs more than one Honey Pot with the same goal as a Honey Pot. Both are used to empirically gather information about how attackers attempt to gain access to a system, Carbone and Geus (2004) being an example. There seems to be significantly less literature that examines how the attackers respond when there is an increase in security. Most tends to be qualitative work such as Rosefeld, Rus, and Cukier (2007) that use Senge's (Senge, et. al. 1994) archetypes as a method to describe attacker-user interaction using simulation.

#### **1.2.5 Utility**

Security imposes a cost on the user. According to Sasse et.al (2001) and Sasse (2003), complex multiple passwords are beyond the capability of human memory. This increases the need for user support which imposes further costs. Recording passwords on paper or automated password retrieval have security and cost issues of their own. These issues have not received enough attention from the security community.

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

### **1.3 Hacker Demographics**

#### **1.3.1 How do you categorize attackers?**

There are several important terms included in the discussion of enforcement as it relates to hacking. Knowing the demographics, and the habits of hackers is important because enforcement often targets the wrong group and sometimes is even set up to apprehend the wrong group or individual (Bilton, 2011).

The economics and politics of hacking make this a numbers game where law enforcement is under significant pressure to show results. Unfortunately, the easiest people to find and the most vulnerable to arrest are those individuals who are the least damaging in terms of their hacking abilities and accomplishments.

### 1.3.2 Hackers

Steele and Raymond (1996) have several definitions of “hackers”:

- “[originally, someone who makes furniture with an axe] n. 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
  3. A person capable of appreciating hack value.
  4. A person who is good at programming quickly.
  5. An expert at a particular program, or one who frequently does work using it or on it; as in `a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
  6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
  7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
  8. [Deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. See {cracker}.”

This lengthy definition is not complete nor is it definitive. The term “hacker” also tends to connote membership in a global community defined by the internet and implies that the person described is seen to subscribe to some version of the hacker ethic.

According to Pekka (2001), the hacker ethic is defined by the following six points:

#### 1. Hands on Imperative.

Access to computers and hardware should be complete and total.

**2. Information Wants to Be Free.**

"Information wants to be free" can be interpreted in two ways. Free might mean without *restrictions* (freedom of movement = no censorship), [or] without *control* (freedom of change/evolution = no ownership or authorship, no intellectual property).

**3. Mistrust Authority.**

Promote decentralization.

**4. No Bogus Criteria.**

Hackers should be judged by their hacking, not by "bogus criteria" such as race, age, sex, or position.

**5. You can create truth and beauty on a computer.**

Hacking is equated with artistry and creativity.

**6. Computers can change your life for the better.**

While parts of this ethos are admirable, much is at odds with main stream American standards that see value in privacy. This dichotomy leads to conflict. Unfortunately, this conflict has shown many hackers a way towards a greater financial reward; and thus, they leave even this loose collection of rules behind.

In the hacker community, it is better to be described as a hacker by others than to describe oneself that way. Hackers consider themselves an elite group, though one to which new members are gladly welcome. There is thus a certain ego satisfaction in identifying yourself as a hacker, but if you are not capable, the community will quickly label you as "bogus" or a "loser" and your credibility will be irrevocably damaged (Lakhani and Wolf, 2003).

Since the 1950s when the term was defined as a practical engineer, the concept of what a hacker is has changed (Brunvand 2000). In the 1960s, the term was first applied to someone who attempted to unlawfully use electronic assets. The "Hacker Culture" may have gotten its start during this period with the Tech Model Railroad Club at MIT (Levy 1984). There are several ways to classify hackers based on their motivation or attack method:

Script Kiddies, Malware Developers, Hactivists, Vigilantes, and state sponsored hacking (Falk 2005).

### **1.3.3 Hacker Demographics**

Examining the motivations of hackers is more complex than it first appears. The hacker population has fragmented into several different groups (Falk, 2005). The following section describes the demographics of hackers and discusses the potential information systems management consideration inherent in being attacked by hackers and crackers. This is important because these different populations have different motivations, skill levels, and resources to use in gaining access to their target system. Their motivation also determines what targets they go after.

#### **1.3.3.1 Script Kiddies**

Those hackers called “script kiddies” do not develop their own tools nor do they have the deep level of system knowledge needed to cover their tracks (McDermott and Fox, 1999). They are similar to juvenile delinquents throwing rocks at windows. The bulk of these “script kiddies” matures and ceases vandalistic behavior as they find other pastimes.

Law enforcement tends to focus on this group because they are not as skilled at covering their tracks as some of the more experienced hackers and tend to brag more about their exploits. This makes them easier to catch. Unfortunately, these are the least destructive in terms of actual hacks. Script Kiddies are also the easiest from which to protect systems. Most common defensive strategies have significant impact on them because they use pre-existing tools that are already in most security software repositories (McDermott and Fox, 1999).

### **1.3.3.2 Malware Developers**

A small proportion of those classified as “script kiddies” continues on to the next step and becomes “malware developers” or “hacktivists”. Malware producers are most often adolescents who are actually developing their own primitive tools.

Most of a malware developer’s motivation is for recognition within his or her virtual community, and most quit after they become adults and after law enforcement professionals begin to hunt them for real. Some few continue to hone their skills and become professional criminals who, while they are still excited by the notoriety, are now hacking for the money (Lee and Bureau, 2007).

A portion of these criminals will eventually “go straight”, often after they are caught, and go into the business of securing the very information they were trying to access. Indeed, the numbers of these professionals are on the rise, indicating that there is a greater market for their services as security professionals or “White Hats” (Caldwell 2011).

Malware developers can mature into professionals and become more skilled at covering their tracks and less inclined to brag about their exploits than their more juvenile counterparts. Often, they are users of “zombie” machines. This tactic involves taking over other computers on the net to cover their tracks. The owners and users of these machines usually do not even know they have been compromised. Malware developers are also turning to viruses as a tool to gain entry into their targets (Richmond, 2004).

Richmond (2004) says that “bots,” which are tools often used to take control of poorly secured systems, are used to infest and control computers. These “bots” come in various specialties and are one of the products that malware developers create.

Building networks of bots, often referred to as “bot nets,” is a profitable business in the underground. There are records of bot nets being bought and sold for the purpose of setting up spam sites. According to Richmond (2004), these are thought to account for one third to one half of the spam that is sent to the average mailbox.

These attackers are much more capable than the Script Kiddies but are also much more easily dissuaded from a specific attack. Their motivation is to get a reputation and therefore, while they will attempt to crack a tough site, they will often abandon it for another that they perceive is less difficult (Lee and Bureau, 2007).

### **1.3.3.3 Hactivist**

The “hactivist” is not really interested in money but rather, has a political agenda. Hactivists use hacking skills to propagate the theme of their activism or to attack the focus of their political agenda (metac0m 2003). In general, hactivists’ computer skills tend to be of a low order. Some hactivists will continue and go from hactivist to cyber-terrorist when they find that nuisance attacks on their targets do not generate success in attaining their political agenda (Hearn, Mahncke, and Williams, 2009).

Hactivists tend to be more open with their efforts, and as a result, these individuals are also more likely to be arrested or otherwise a target of enforcement. Those few that make the move to cyber terrorist become very secretive and difficult to arrest. Many of these former hactivists will become members of state sponsored hacking organizations if the nation state in question aligns with their goals.

Their motivation is to get notoriety for their cause, so a tough site to crack will often be abandoned for another from a similar group of targets; hacking one oil company is pretty much like hacking another in their eyes. Beating this class of hacker is similar to beating the



malware developer in that the system administrator doesn't need airtight security, just better than average for the peer group.

#### **1.3.3.4 Vigilante**

Another offshoot of the hacktivist tree is the vigilante, one who is involved in investigating potential criminal activity that is, in his or her opinion, being underreported or investigated. While vigilantes break the law and enter restricted systems, their goal is not usually monetary or destructive to the integrity of the system (Falk 2005).

This group is rarely a serious target for enforcement because they tend to hack to show people how vulnerable the target system is. Vigilante humor is often crude; the goal is usually not to bring something down, but to make a site more secure.

Vigilante motivation is to investigate what he or she perceives as criminal behavior of a given organization, so a tough site to crack will often be abandoned. Indeed, they focus on the weakest site of a particular target group. Again, beating this class of hacker means you don't need airtight security, just better than average for your peer group.

#### **1.3.3.5 State Sponsored Hacking**

A very small percentage of all forms of hackers move on to state-sponsored cyber warfare units. These units are made up of both hackers and security professionals. The hackers are rarely in positions of authority and are very closely supervised by the more formally trained members of the staff. For example, the United States Air Force has paid a security firm to build a virtual town to prepare our own government hackers to engage in cyber warfare (Kelley 2012). They also have deployed 13 teams to carry out offensive cyber warfare (Mazzetti and Sanger 2013).

State sponsored hackers are almost completely beyond the reach of all but the most vigorous enforcement. Many governments deny the existence of state sponsored hackers but still use them. The Chinese government has recently denied the fact that they aid in cyber-attacks while supporting them (Mozur 2013). As the stakes are very high, any security action against this class of hacker merely slows them down from their eventual goals because the governments shield them and set their objectives.

State sponsored hacking is becoming more prevalent partially because hacking is also becoming more international. The United States is still the most common place a hacker will be found, but its share fell to 37% from 58% recently. China rose to No. 2 from No. 3, switching places with Canada. Enforcement and extradition are notoriously hard across these national borders.

Defense against this sort of hacker is much more difficult and often requires an active offense to dissuade the attacks. Since their objectives are set by outside entities, they will often continue to attack a well-defended system. They can be very persistent. Extraordinary measures such as Honey Pots (Schwabel, Rohring, Hall, and Scultz, 2000) and other forms of misdirection can be very valuable in aiding a defense against state sponsored hackers.

#### **1.3.3.6 The Professional Criminal**

There are hackers motivated by personal economic goals. They are often called professional criminals and respond to the size of the reward and the ease at which that reward can be obtained (Richmond 2004). In this sense, they are similar to the rational criminals described by Becker (1968).

Richmond's (2004) article supports the thesis that there is a large population of "for profit" attacks on information systems. "For profit" attacks also suggest that these are rational criminals.

Their motivation is economic and rational, so a tough site to crack will be abandoned for another from a similar group of targets. They don't care about any specific target, only that they can reap the largest reward in the shortest time.

Both state sponsored hacking and professional criminals utilize "social engineering." In other words, these attackers interact with people who use or defend the information system in question in order to get either intelligence about how to crack the system or to get at the information they need (Mitnick and Simon 2002).

Succeeding against this class of hacker is similar to dealing with a malware developer in that you don't need air tight security, you just need significantly better security than average for similarly valued targets. The difficult portion is determining your peer group.

#### **1.3.4 Hacker Life Cycle**

Publicly available data suggests that the number of hackers varies over time. While determining what constitutes a hacker is open for debate, there is some evidence that the hacker population is undergoing constant turmoil (Ksjetri, 2006).

#### **1.3.5 Hacker Longevity**

Taylor (1999) describes the hacker population of the 1990s as predominately male and young (teens through 20s with a few outliers in their 30s). Turgeman-Goldschmidt (2005) did a series of interviews with 54 Israeli hackers, who were also predominately male and young, with a median age of 25. Adam (2004) describes a society of young males and cites several authorities that attest that this was the norm of the hacker population at least as

far back as the 1980s. If that is the case, then to maintain a young population, new individuals are constantly joining the group as older individuals either leave the group or, in rare cases, are arrested.

It appears that hackers move through the various populations with ease. While some script kiddies grow up to be high end hackers, the bulk of the criminals have technical backgrounds. The hactivists also tend to be more insular, gaining initial skills from the web. They obtain more capability by either persuading university students who follow their causes to help recruit the technical people they need or developing the skills themselves (Taylor, 2005).

### **1.3.6 Hacker Groups**

The informal groups that hackers congregate in are tenuous and ephemeral. Jordan and Taylor (1998) describe hacker circles that, when one member has been arrested, disappear; members either stopping being hackers or adopting a low profile. This same paper also quotes an interview with a member of the “Legion of Doom,” a well-known hacker’s organization. This particular hacker said if you lay off hacking for a few months and then come back to the group, almost everyone is new. Clearly, the population of hackers is in constant flux.

When the members of the group “Anonymous” were arrested in 2012, the oldest was twenty-nine and the youngest was seventeen. The group’s undoing was infiltration by Interpol (Satter, 2012). Infiltration was easy because the membership of this group was not structured and because members self-identify. Some of those arrested had only been affiliated the group for four months (Olson, 2012).

### **1.3.7 Basic Approach**

This research focuses attention on the societal value of the information system using a utility function about which only limited assumptions are made. In this context, it means looking at maximizing system value rather than maximizing security or minimizing attacks. It also translates into response functions which are inherently inexact. Such ambiguity it seems is inherent in this approach. Block and Heineke (1975) use one term to represent the “failure, capture, or arrest rate” with criminal behavior and show how soft the definition of similar terms in related work can be. This does focus attention on aspects of the problem that are not well understood and therefore suggest fruitful avenues for future research.

It is clear that attacks on a system reduce its value. While the value of the organization that has constructed the information systems is only part of the commonly held notion of value, there is evidence that firm value can be reduced by cyber attacks (Garg, Curtis, and Halpner 2003; Miora and Cobb 1998; Saita 2001, Olavsrud, 2001)

## **1.4 Research Question**

In order to properly allocate scarce personnel, funds, and equipment, computer scientists need a better understanding of how hackers respond to security measures and how to model this behavior in complex information systems. Much of the information used in making decisions is subjective. The knowledge available about attackers’ responses needs to be quantified if the desire is to move attacker profiling from an art to a science. The following are the hypotheses for this research.

### **1.4.1 First Hypothesis**

The null hypothesis ( $H_0$ ) is that there is no relationship between the attack rate and the effectiveness of security measures. The alternative hypothesis ( $H_1$ ) is that there is a

relationship between attack rate and the effectiveness of security measures and that the curve representing the response is “S” shaped.

#### **1.4.2 Second Hypothesis**

A second focus of this research is based on system value. The null hypothesis ( $H_0$ ) is that there is no relationship between the attack rate and the value of the information system. The alternative hypothesis ( $H_1$ ) is that there is a relationship between the attack rate and the value of an information system and that the curve representing the response is “S” shaped.

## Chapter 2. General Simulation Model

This chapter was compiled and expanded from a paper by Pendegraft and Rounds (2007). It describes the theoretical model that drove this research. The approach in previous work (Pendegraft, Rounds, and Frincke (2005), Pendegraft, Rounds (2006), and M. Rounds, N. Pendegraft, and C. Taylor, (2007)) relies upon Senge (1990) who in turn drew from Forrester's work at MIT on systems dynamics modeling (1961). This approach takes a top-down point of view.

### 2.1 Computer Security Problem

For the nine most recent years surveyed by the US Census, the revenue generated through e-commerce has increased each year. Further, the rate of increase is itself increasing. In 2000 \$28.35 billion in revenue was generated by e-commerce in this country. In contrast, 2013 3<sup>rd</sup> quarter revenue was over twice as large as all of 2000 at \$67.1 billion. In 2002 \$43.5 billion and for last year surveyed "2003" \$54.9 billion was generated. In 2004, e-commerce made up just 2% of total retail sales. In 3<sup>rd</sup> quarter 2013, the figures was over 5.6%. This includes only e-commerce, not those business functions that are supported by networked systems but have not been given a monetary value.

The threat against e-commerce is also on the rise. A defacement attack on e-commerce sites is one of the easiest types of attacks to measure and hence what is used in this case as a proxy for the total attack rate. For example, according to Artisoft (2001) the number of defacement attacks in 1999 was approximately 3,000; in 2000 the number jumped to 6,000; in 2001 the number significantly increased to 30,000. This trend continued and in 2010 there were almost 1.5 million defacement attacks (Vympel and Minor, 2011).

While the amount of money spent on computer security has increased, it has not kept up with e-commerce revenue. According to the Fredonia Group (Security Systems News, October 2002), spending in this country on security related issues for 2000 was approximately \$2.64 billion; in 2001, it was approximately \$2.9 billion for a 10% increase. In 2002 the spending was approximately \$3.4 billion, an 18% increase, showing significant post 9/11 increases. For 2013, spending was projected to be \$93.6 billion for an annual increase of just 8.33%. The computer security community is being asked to protect ever more valuable assets with relatively less (Thoras, 2013).

The problem of computer security is not going away, and the research cited shows that the value of e-commerce is increasing and that the resources to protect the rapidly expanding e-commerce market are being spread ever more thinly. This being the case, it becomes apparent that allocation of these scarce resources is a significant problem.

## **2.2 Methodology / Simulation Background**

Similar approaches to simulating the human factors and organizational information have been used by Dutta and Roy (2008), who view the construct of value as a reservoir. Martinez-Moyano, et al. (2008) use this systems dynamics modeling to examine insider threats to an organizational information system. Rosenfeld, Rus, and Cukier (2007) examine the use of Senge's (1990, 1994) archetypes in examining human/information system interaction.

Systems dynamics models use two types of objects, reservoirs and flows, to describe feedback relationships in complex systems. Reservoirs represent constructs whose values change over time, and flows represent changes in the values of those constructs. The flows are, in effect, derivatives of the reservoirs. The models cited are simple because, as Senge



(1990) point out, simple models are much easier to understand. There is also the problem of exploding state space as models become more complex.

It has also been assumed that the security decisions and perceptions of value are continuous in nature. While security decisions are at least partially discrete, Rajput, Chen, and Hsu (2005) demonstrate that security decisions are being broken up into ever smaller increments as the users are given more and more options as the systems become more refined and complex. The result is that security choices are reasonably continuous.

The specific model used in this dissertation is a reservoir-flow model similar to that introduced by Forrester (1961). He used stock and flow models to investigate the behavior of industrial systems involving feedback. He argued that experimenting with models of such systems via simulation permits examination of implications of policy decisions. During the ensuing 40+ years, simulation has become recognized as a powerful way to study systems (Winston 1994).

Senge (1990) studied the behavior of complex systems and offered several “archetypes” for complex interactions. Building the model for this dissertation is similar to Senge’s “Limits to Growth” model. In particular, he discussed the implications of delayed feedback on systems. It is often the case that delayed feedback loops result in highly complex behaviors.

In such models, there are two types of object: reservoirs and flows. Reservoirs represent constructs whose values change over time, and the flows represent changes in the values of the reservoirs. In effect, the flows are derivatives of the reservoirs. In the current research for example, a reservoir was used to represent the value of the information system (IS). The flows represent changes to the value of the system based on both use of the system

and attacks on the system. In general in this model, use of the system results in an inflow, increasing the value of the IS, and attacks result in an outflow, decreasing the value of the system. The IThink application (High Performance Systems) transforms the model into a set of finite difference equations which are solved iteratively.

The graphical model similar to Senge (1990) was used rather than the differential equation model like Becker (1961) because the investigators believe that it is easier to understand, and it is easier to extrapolate the behavior of the system via simulation. Further, simulation makes it possible to study the behavior of systems of differential equations which cannot be solved in closed form. Senge's caution that a model not be made too complicated was heeded. The investigators concede the simplicity of the model, yet it produces interesting and informative behavior. It makes no sense to construct a more complete (and therefore complex) model until one can fully understand the simple model.

## **2.3 The Model**

### **2.3.1 Conceptual Background**

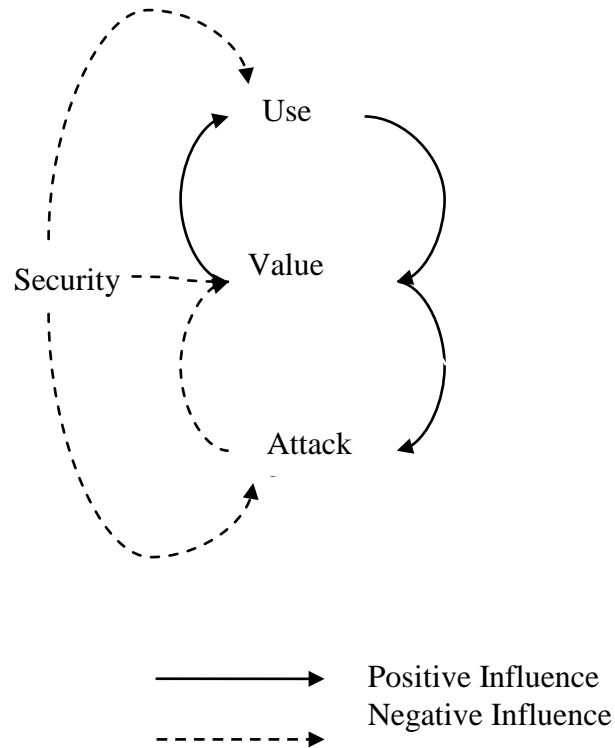
Our model depends on four fundamental constructs: VALUE, USE, ATTACKS, and SECURITY. These are inherently fuzzy terms, and the investigators deliberately do not attempt rigorous definitions in this paper. Clarification of these constructs is planned for future work. The VALUE construct is a reservoir. USE and ATTACKS are flows, and SECURITY is a control parameter representing the management decision. The major decision that management makes is how much of their scarce resources to spend for Security. Resources spent here, necessarily means that they are not spent doing things that the company is in business for, reducing the potential value of the firm.

SECURITY also decreases value because information system assets are often harder to use. For example a longer password is harder to use and using firewalls can increase response time and impact connectivity. These costs are harder to estimate but according to Pasquali (2013) they are very real in terms of the bottom line.

VALUE subsumes several distinct elements of the ISM (Information System Success Model). In particular, the issues of system and data quality are combined which are held distinct in the ISM. In addition, VALUE includes aspects of firm value per Zhu and Kraemer (2005). Separating these notions of value in the model presents an interesting opportunity for future work. The revised ISM model suggests that increases in VALUE lead to further USE. Zhu and Kraemer show that use leads to increases in firm value, and it seems clear that legitimate use of an information system increases the system's value. For example, adding records to a database or correcting errors in a database, both common uses, increases the value of that database. Hence, it is assumed in the model that increases in VALUE lead to increases in USE.

These models link these two constructs through intermediaries which are omitted in this dissertation in the interest of simplicity. The investigators justify these simplification on the grounds that the more detailed links supported in the empirical literature would add little insight at this point in the work. Further, including them would substantially increase the complexity of the model. Thus, the model assumes a macro perspective while leaving substantial room for additional work to bring it into closer alignment with the empirical literature.

VALUE includes properties such as data quality, data volume etc. VALUE is increased by USE which is in turn increased by VALUE. However, increased system value also increase attacks which in turn decrease value (Figure 2).



**Figure 2. Basic Model**

To ease the development of the mathematics, the notation is simplified in the following. Let  $V$  be the system value (VALUE in the computer code).  $V$  is assumed to change additively due to use and attacks. In a particular time interval  $\Delta V = R * U(V, S) - A(V, S)$  where  $S$ ,  $U$ , and  $A$  are SECURITY, USE, and ATTACKS respectively and are of the form noted below.  $R$  is a measure of the relative importance of use compared to attacks.

Also assumed is that users and attackers constitute two internally homogeneous groups. Each group is described in terms of a representative agent. The behavior of the representative agents is described by their utility functions:

$U(V, S)$  = level of use and

$A(V, S)$  = level of attacks where

$V$  = system value

$S$  = security level.

Further it is assumed that these functions are multiplicatively separable:

$U(V, S) = F_{UV}(V) * F_{US}(S)$

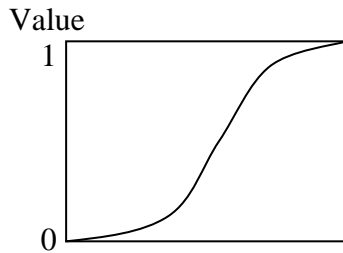
$A(V, S) = F_{AV}(V) * F_{AS}(S)$

$F_{UV}$  and  $F_{US}$  are assumed to be S shaped as discussed below.

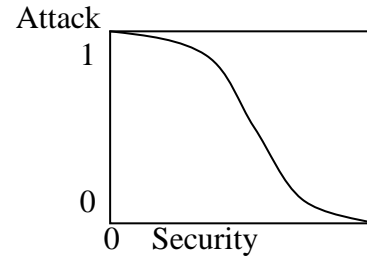
Figure 3 typifies  $F_{UV}$  and  $F_{AV}$ . First the investigators assumed that USE is positively influenced by value. Second, it is assumed that for low values of  $V$ , there will be little use beyond the minimum mandated by management. But, as value approaches and then exceeds some critical value,  $V'$ , use will increase rapidly, being highly sensitive to  $V$  at the margin. At some point, use will taper off.

Figure 4 shows the shape of typical  $F_{US}$  and  $F_{AS}$  responses. The investigators assumed that low levels of security do not impact the user and hence there is little effect,

however as security climbs, it has more impact on the users so USE and ATTACKS decrease.



**Figure 3. Value vs. Use and Attacks**



**Figure 4. Attacks vs. Security**

The idea that the responses are “S” shaped, while an assumption on the investigator’s part, is supported by Yamada, Ouba, and Osaki (1983). This behavior was modelled with a piecewise exponential function which ranges from 0 to 1:

$$F_{UV}(V) = \begin{cases} -1 + \exp(MVU * (V - VU')) & \text{for } V \leq VU' \\ 1 - \exp(MVU * (VU' - V)) & \text{for } V > VU' \end{cases}$$

So, each agent’s reaction to value is determined by two values.

$VU'$  determines the point of inflection and

$MVU$  determines the steepness of the curve.

In similar fashion, it was assumed that agents have negative utility for security. This is the case for attackers and for employee users for whom security is a burden. Hence, customers who are attracted by security are excluded from examination. These users will be a focus of future study. These functions also range from 0 to 1.

$$F_{US}(S) = 2 - \exp[MSU * (S - SU')] \text{ for } S \leq SU'$$

$$+ \exp [\text{MSU} * (\text{SU}' - S)] \quad S > \text{SU}'$$

The attacker is described in a similar fashion.

$$F_{AV}(V) = -1 + \exp [\text{MVA} * (V - \text{VA}')] \quad \text{for } V \leq \text{VA}'$$

$$1 - \exp [\text{MVA} * (\text{VA}' - V)] \quad V > \text{VA}'$$

and

$$F_{AS}(S) = 2 - \exp [\text{MSA} * (S - \text{SA}')] \quad \text{for } S \leq \text{SA}'$$

$$+ \exp [\text{MSA} * (\text{SA}' - S)] \quad S > \text{SA}'$$

Thus to fully characterize each agent requires four parameters:  $V'$ ,  $MV$ ,  $S'$ ,  $MS$  for a total of eight parameters. The size of the state space was reduced by fixing the attackers' parameters, and defining the users' parameters as ratios with respect to the attackers' values.

It is acknowledged that it is a strong assumption for both attackers and users to be homogeneous. There are professional crackers who are motivated by profit and amateurs who are doing it for notoriety. In the user community, there are trusted users who rankle at all security and users who value a modicum of security. In this model it has been assumed that users will work with a reasonable amount of security and that attackers are drawn primarily by value. These are strong assumptions and it is intended that this will be relaxed in future work.

### 2.3.2 IThink Model

The simulation model was built with IThink and is illustrated in Figure 5. The equations of the model are listed in Figure 6. The reservoir (rectangle) represents system VALUE. Its value can change depending on the inflows and outflows indicated by large arrows. The flow on the left (USE) causes increases in VALUE. The flow on the right (ATTACKS) is an outflow which decreases VALUE. The drain was included to model the possibility that VALUE might naturally decrease over time as data and technology become obsolete.

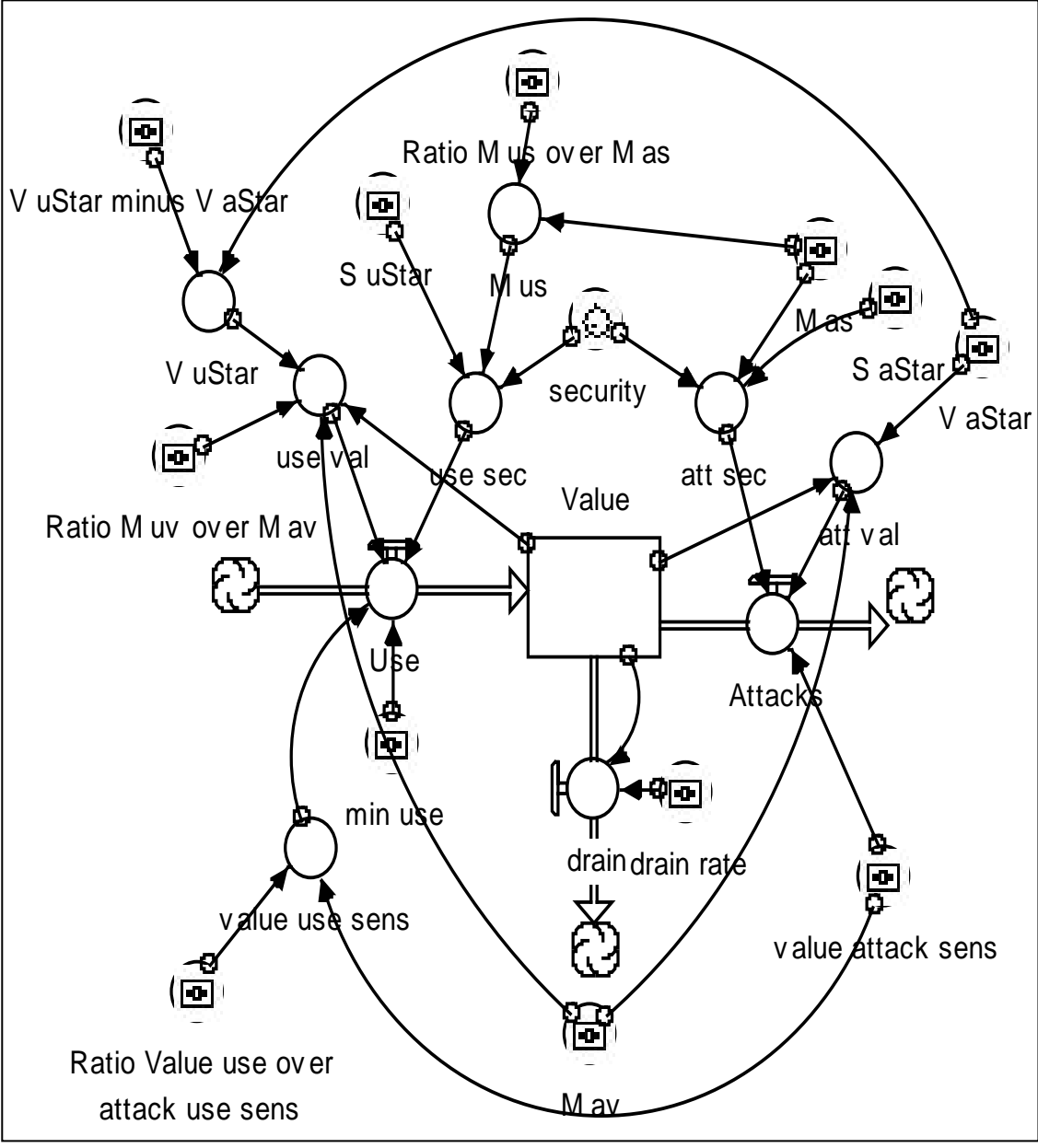


Figure 5. Ithink Model

$$\text{Value}(t) = \text{Value}(t - dt) + (\text{Use} - \text{Attacks} - \text{drain}) * dt$$

INIT Value = 1000

INFLOWS:

$$\text{Use} = (\text{use\_sec} * \text{use\_val} + \text{min\_use}) * \text{value\_use\_sensor}$$

OUTFLOWS:



```

Attacks = att_sec*att_val*value_attack_sensor
drain = delay(Value,1)*drain_rate
      att_sec = 1+(if (security-S_aStar<0)
                    then 1-exp(10*M_as*(security-S_aStar))
                    else -1+exp(10*M_as*(-security+S_aStar))
                    )
)

att_val = 1+(if (Value-V_aStar<0)
               then -1 + exp(M_av*(Value-V_aStar))
               else 1-exp(M_av*(-Value+V_aStar))
               )
)

drain_rate = 0
min_use = 0
M_as = .2
M_av = .0003
M_us = M_as*Ratio_M_us_over_M_as
Ratio_M_us_over_M_as = 1
Ratio_M_uv_over_M_av = 1
Ratio_Value_use_over_attack_use_sensor = 1
security = 0.1
S_aStar = .5
S_uStar = .5

use_sec = 1+(if (security-S_uStar <0)
               then 1 -exp(10*M_us*(security-S_uStar))
               else -1+exp(10*M_us*(-security+S_uStar))
               )
)

use_val = 1+(if (Value<V_uStar)
               then -1 + exp(Ratio_M_uv_over_M_av*M_av*(Value-V_uStar))
               else 1-exp(Ratio_M_uv_over_M_av*M_av*(-Value+V_uStar))
               )
)

value_attack_sensor = 1
value_use_sensor = Ratio_Value_use_over_attack_use_sensor*value_attack_sensor
V_aStar = 1000
V_uStar = V_uStar_minus_V_aStar+V_aStar
V_uStar_minus_V_aStar = 0

```

**Figure 6. Model Equations**

After some experimentation, the inflection points were settled upon in the security response curves (SA\*, SU\*) as primary state variables. This simplification greatly reduces the size of the parameter space and still results in a rich set of behavior. In the Model these

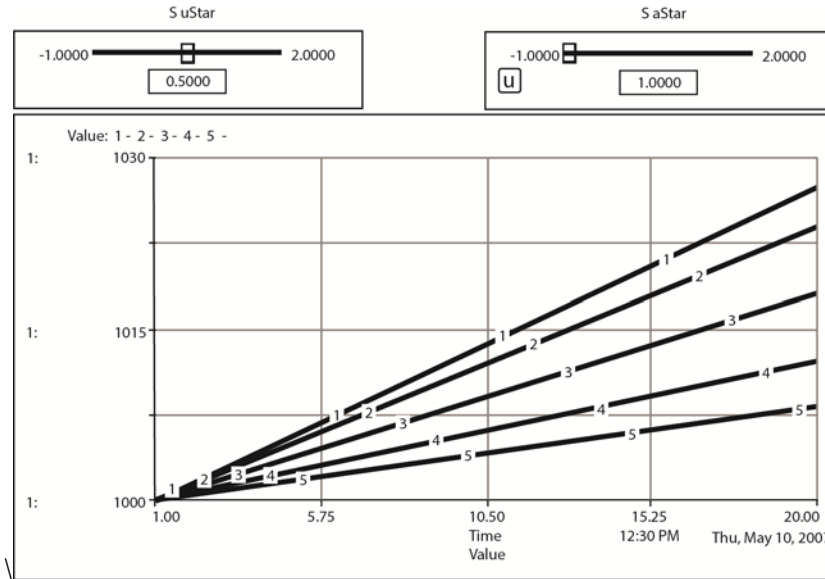
parameters are labeled  $S_a\_Star$  and  $S_u\_Star$ . Several parameters as pairs with the attacker's value fixed and the user's value is expressed as a ratio with respect to the attacker's value. For example, MAS is fixed at .2 and MUS is determined by the value of the parameter RATIO MUS OVER MAS. In most cases in the current model, this ratio is set equal to 1, reflecting the two parameters being equal. This format made it possible to, in effect, reduce the side of the state space. The fixed value (.2) was chosen arbitrarily.

The state variables can be varied by the sliders, which in IThink are graphical controls to adjust parameters in the model, and the level of security can be controlled using the dial. The dial works in a similar manner to the slider but in a rotary fashion. The sliders are used to set the environmental state by identifying the sensitivity of the users and attackers to security and to system value. It is important to emphasize that the various constructs are not intended to measure in specific units any particular system property. Rather, they represent general notions related to the indicated concepts.

## **2.4 Discussion of Model Results**

Four Basic responses were observed (see Figures 7, 8, 9, and 10). The graphs show the VALUE of the system over time for values of security ranging from .1 to .9 in steps of 0.2. Runs are numbered consecutively; thus run #1 has security = 0.1, run #2 has security = 0.3 and so on. Thus they show the change in value over time ( $\partial V/\partial T$ ) and the change in value with respect to security ( $\partial V/\partial S$ ). The results show that there exist conditions in which  $\partial V/\partial T$  and  $\partial V/\partial S$  can be either positive or negative. This suggests that there may be two classes of users (and attackers) whose behavior is similar to that of early and late adopters (Rogers 1976).

Figure 10, which shows increasing system value and increasing returns to security in the extreme, shows when  $Su^*$  is large. In other words, the users are largely unaffected by the security in question, while the attackers are.



**Figure 7.  $Su^*$  is Large, (+,-) Value is Increasing, Security is Detracting from Value**

By contrast, Figure 8 shows a system in which  $Sa^*$  is large. Here the attacker is unaffected by the security available while the user is. This results not only in negative changes in system value, but in negative returns to security as the increased security does not affect the attackers, but does drive users from the system.

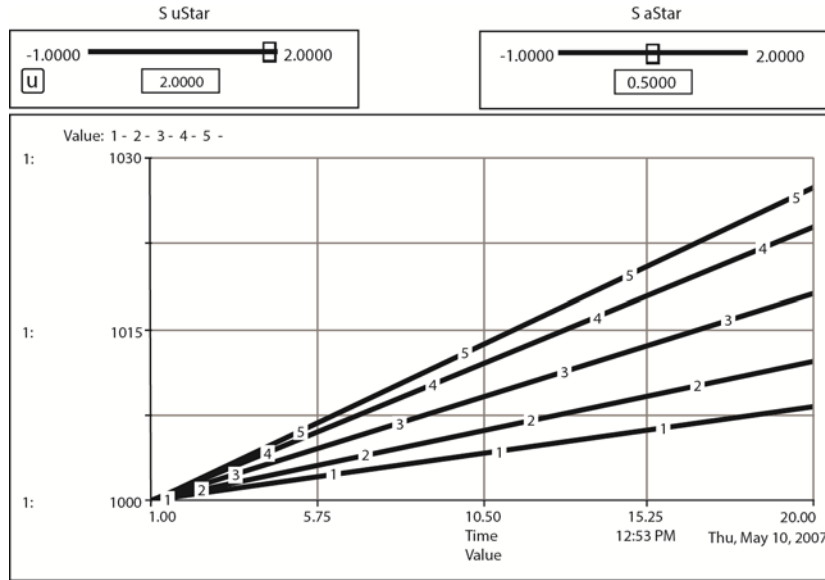


Figure 8. Sa\* is Large, (+,+) Value is Increasing, Security is Enhancing Value.

Figure 9 shows a situation where systems value is declining but additional security lessens the decline and Figure 10 show a situation where the decline is aided by additional security.

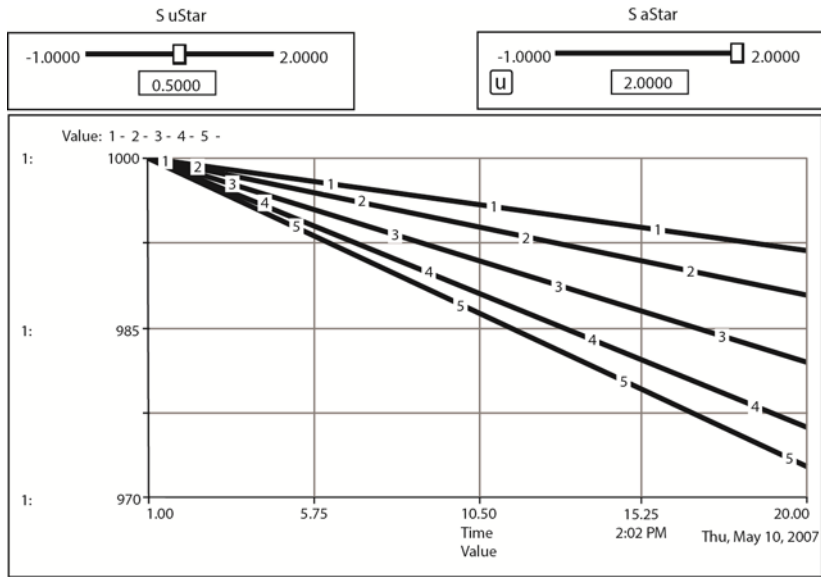
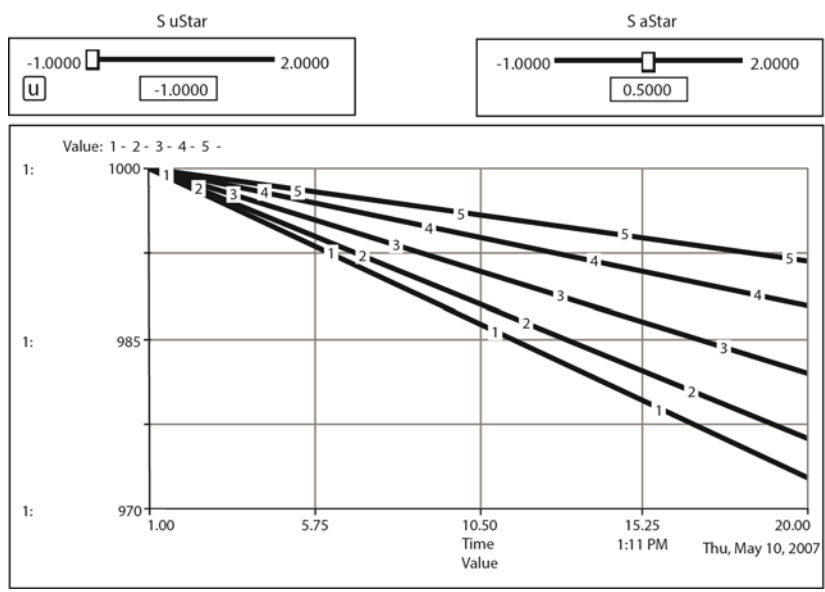
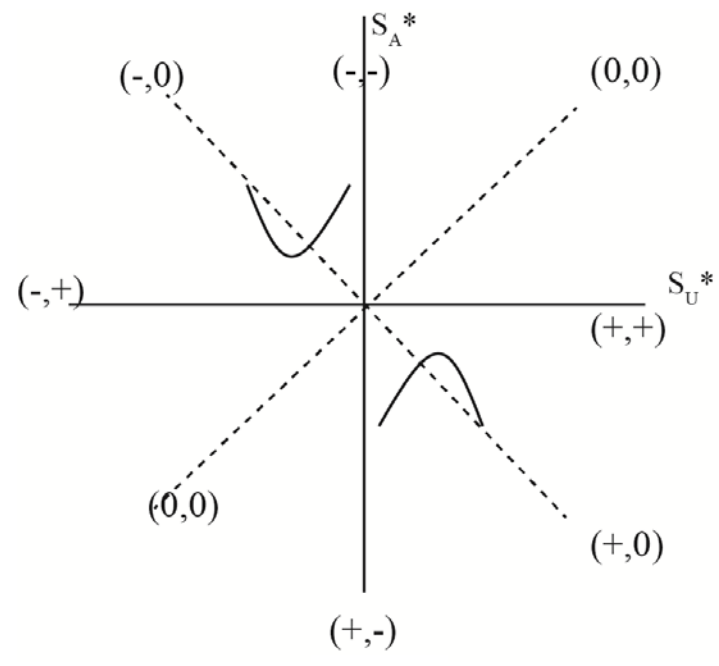


Figure 9. Sa\* is Large (-,-) Value is Decreasing, Security is Detracting from Value.



**Figure 10.  $S_u^*$  is Small (-,+)  
Value Decreasing but Additional Security Lessens Decrease**

In order to better understand what is happening, several more extreme cases were investigated and plotted the response as a function of  $S_A^*$  and  $S_U^*$ , in effect treating  $S_A^*$  and  $S_U^*$  as state variables. The graph in Figure 11 illustrates these findings. **Figure**



**Figure 11. Response Graph**

In each of several extreme cases the behavior was characterized with a tuple whose elements are +,0, or -. The first element of the tuple indicates the sign on the slope of the Value vs. Time curve, i.e.  $\partial V/\partial T$ . A 0 indicates that there is no change over time. Similarly the second element in the tuple gives the sign of  $\partial V/\partial S$ ; similarly, 0 indicates no change with respect to S. Thus in those regions with  $\partial V/\partial S > 0$  it makes sense to increase security. In those with  $\partial V/\partial T < 0$ , there is a system problem since the value of the system is declining over time. These occur in regions of low  $SU^*$ , that is regions in which users are very sensitive to security. Thus, the correct response is to shift the user's response curve to the right by reducing user sensitivity through training or adopting less intrusive security measures.

In the central region of the graph both attackers and users are responsive to changes in SECURITY. Here more complex behavior was observed. The response in Figure 11 shows that the value of the system increases with SECURITY for a while and then begins to decrease with increased SECURITY. The response to SECURITY is concave, hence the concave curve on the graph. Thus, there is an optimal level of SECURITY. In this case the value is approximately 0.3. Security managers in this sort of environment need to be sensitive to the marginal impact of any changes they make, increasing security until the marginal return is negative.

Similarly in the region identified by a convex curve, at low and high levels of SECURITY, VALUE is high, but it decreases for middle levels of SECURITY. Managers in this region should select either high or low levels of security. It is not clear from this level of analysis which would be of greater benefit. Figure 12 shows a situation where the response

is concave. Similarly, Figure 13 shows a situation in which the response is convex. Figures 13, 14, and 15 respectively show conditions labeled (0,0), (+,0), and (-,0) in Figure 10.

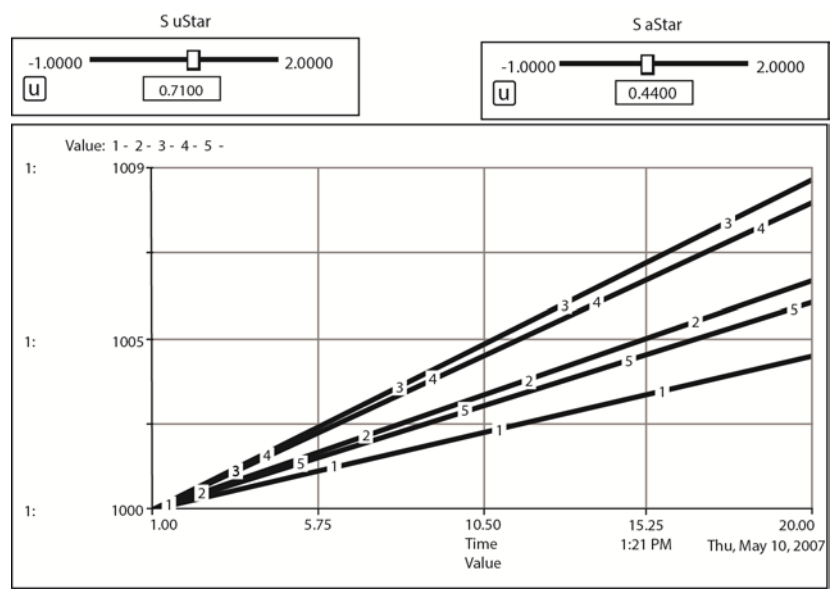


Figure 12. Response is Concave, Value Increases to a Certain Point and then Decreases

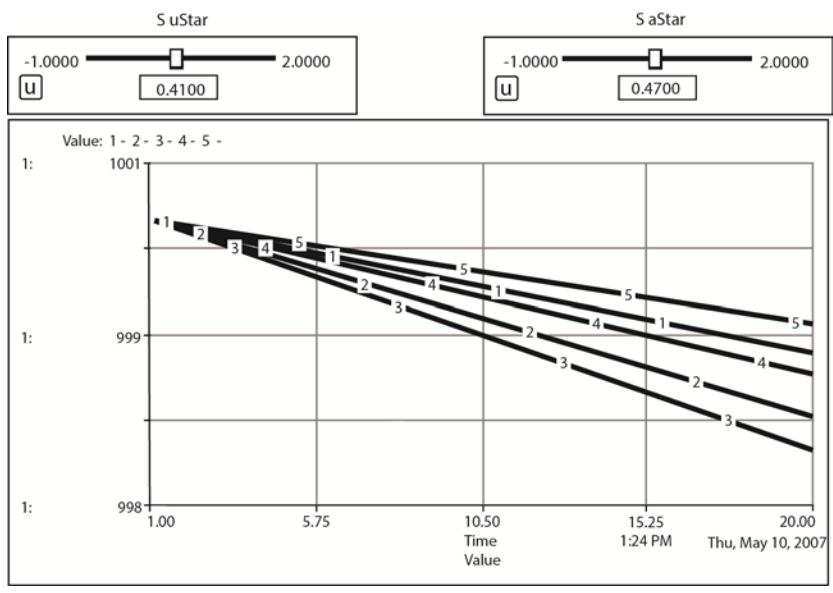
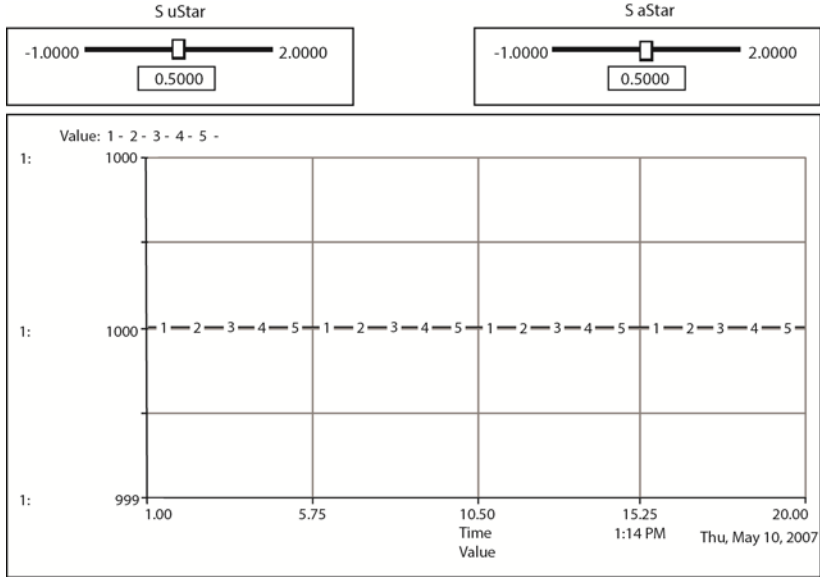
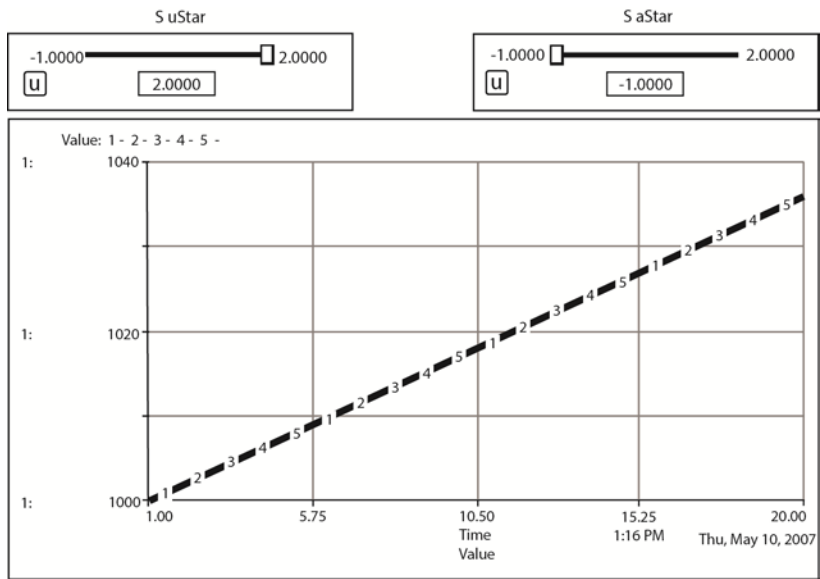


Figure 13. Response is Convex, Value decreases to a Certain Point and then Increases

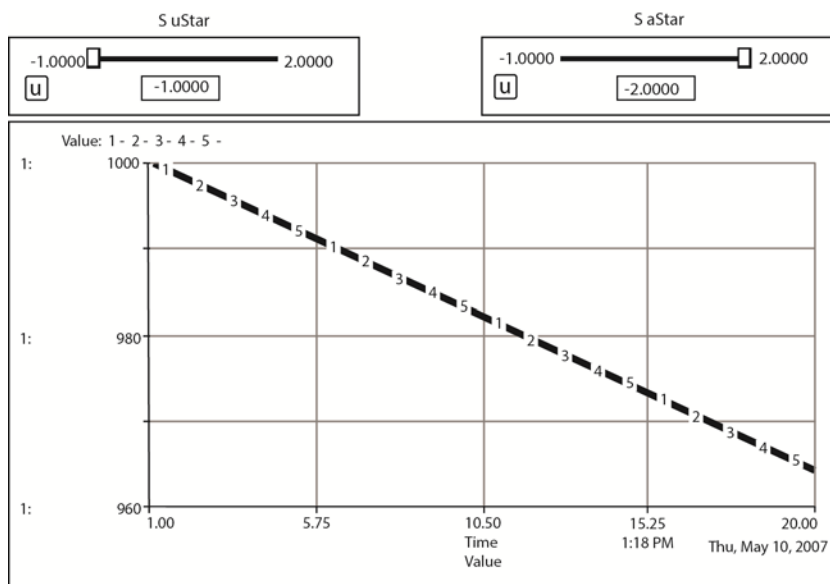


**Figure 14. (0,0) Value and Security Remain Unchanged**



**Figure 15. (+,0) Value Increases but is not Effected by Changes in Security**





**Figure 16. (-,0) Value is Decreasing but not Effected by Security**

The clear implication of this result is that system managers need to be aware of their locations in the state space, since selection of the correct policy is dependent on the location of the system in the state space of Figure 10. One policy implication is immediately apparent: in those regions where  $\partial V/\partial S < 0$  it makes sense to change the state, perhaps by educating users, rather than to increase security. In particular, while Security Use Sensitivity has been taken to be a fixed value, it may in fact be subject to influence. For example, training might make users less sensitive to security. Perhaps simplifying the security system by use of single sign-on or biometrics might also make users less sensitive. In states where  $\partial V/\partial S > 0$  it makes sense to increase security in conventional ways.

Further, the results may be applied to situations in which the manager does not have complete control over security. Letting SECURITY range from 0 to 1 maps into the security options available to the manager, but still allows for other security measures to be in place, or not be available at a particular level.

The model has shown sufficient validity to be worth extending. For example, VALUE is probably more complex. In particular, it may be a function of system value and rate of use. As noted above, the notion of VALUE contains aspects of system value and firm value. In essence it is assumed that these values are tightly related. This model also assumes that legitimate users and attackers will use similar metrics for VALUE. These are strong assumptions and will need to be relaxed in subsequent work. Similarly, it is assumed that all users will be deterred by increased security, while it is likely that some customers will in fact be attracted by increases in security as in the case perhaps of a bank or other lending agency. Similarly, SECURITY is also fuzzy. Explicating these issues remains to be done.

The models may also be extended in other ways. For example non-homogenous attackers might be included such as so called crackers and hackers with differing motives. Falk (2005) breaks hackers into five categories relative to the moral reasoning they employ. Their modes of attack, focus, and intent are all different. Jordan and Taylor (1998) also describe a variety of motivations. These differences in motivation could be incorporated in future simulation designs to enhance the accuracy of the model and help define the concept of value.

The early/late adopter model of user behavior should also be examined. It is also believed by the investigators that there are various classes of attackers each with a specific response curve and inflection point. These different populations can be modeled and have predictive value. The current model assumes static users and attackers; that is, their characteristics do not change over time. This is a strong assumption, which can be relaxed in future work. It has also been noted that there are certain similarities between the two major classes of users and marketing research on Early Adopters vs. Late Adopters (Rodgers, E.,

1962) of a new product. This is clearly a linkage that needs to be researched. As such, this model is dynamic in nature and will be continually modified. All of these various refinements introduce considerable complexity into the model. A path of stepwise refinement of the model with evaluation at each step appears to be the prudent approach.

## **Chapter 3. Experimental Methodology**

### **3.1 Research Direction**

This dissertation evaluates the shape of the curve when comparing the number of attacks to system value and system security through a series of three experiments.

The first experiment varies the level of security. The value of the security task and therefore the value of the system will remain constant. These curves can be characterized by a controlled laboratory experiment where a student's responses create increases in security and increases in value of the target.

The second experiment keeps the level of security and hence the security task constant but varies the reward utilizing the same methodology.

The third experiment is a repeat of the first with a higher reward level and a different recruiting strategy for the participants.

### **3.2 Experimental Design Background**

The purpose of these experiments is to support or reject the assumption that the curves for attacker responses to security and financial reward are "S" shaped. It is clear that this is not one experiment but a series of experiments. It is possible to design one software environment to handle them all, but it is critical not to try and do too much at each step. In this series of experiments, the measurements of attack rate, number of successes, and the number of participants has been used to examine and operationalize the concept of attack rate.

The methodology of designing economic experiments to explore markets and other phenomena began very early in the study of economics (Bernoulli, 1738), but the real use of

the technique to examine individual choice started in the 1930s (Thurstone, 1931) and 1940s with Wallis and Friedman's (1942) critique of that experiment.

Rousseas and Hart (1951) designed an experiment to reply to Wallis and Friedman's critique with a more concrete and realistic treatment of the decision, in this case, different breakfast menus. Also Mosteller and Noguee (1951) examined how people valued additional income which has bearing on this experiment.

Kagel and Roth (1995) have described the current thought in this methodology and Plott and Smith (2008) have expanded on it in their Handbook of Experimental Economics. It is Plott and Smith's ideas that have guided this research.

### **3.3 Validation of Methodology**

Plott and Smith (2008) have collected and summarized the literature and practice on the subject of experimental economics in regards to examining individual choice into a handbook. Becker (1968) explored motivation and behavior when relating crime and economics. Schram (2000) has broadened the knowledge of the motivations and behaviors of various actors in economic decision making. Karlan (2005) says that experimental labs can reflect real world behaviors. Alm (1991) reviews similar research on tax evasion that indicates that people pay taxes primarily because they fear enforcement. The results from both of these experiments mirror observed behaviors in the real world.

Lum and Yang's (2005) results show that there is general support in the theoretical community for experimental economic research as it relates to crime and punishment. Research is limited by funding pressures as well as academic mentorship issues that guide researchers away from this method. Lum and Yang (2005) also say that the research and the

results appear valid, but that social pressures tend to push researchers away from this technique.

Jonsson and Olovsson (1997) conducted an experiment using human subjects (students) to examine the security intrusion process. Students were used as proxies in this research for both attackers and users to replicate real life situations. Their results suggest that there is distribution of frequency and motivation to attacks and that perhaps current reliability models such as Sengi et. al. (1994) can shed some light on attacker behavior. This paper also makes a good case concerning the issue of students used as a proxy for stakeholders in an information system.

Christin et. al. (2011) conducted experiments that incentivized users to run potential malware and concluded that users will run potentially harmful software if the incentive is great enough.

### **3.4 Methodology Background**

The methodology used in this research is defined as an “observational study” (Rosenbaum, 2002) and uses no control group. It can also become unfocused and hence not return useable results unless the scope is kept small. Therefore, the number of subjects was limited to stay within available funding and to keep the data set manageable. The literature (Grossklags 2007) indicates that, in similar experiments, trial groups of a minimum of four and a maximum of twelve are sufficient. Properly managed, the number of subjects can be kept in a feasible range without affecting the research reliability. The experiment was designed to be repeatable so that if more trials were needed after the initial data have been evaluated, they can be run in a similar manner.

The security task used was “cracking” a “password.” The system was designed to vary the length of the password and the size of the “alphabet”. The ability to vary both the length of the password and the size of the alphabet provided a very fine grained control of the difficulty of the security task as it was possible to closely control the number of possible passwords and hence the security difficulty.

Although this task is not similar to current password cracking techniques, we believe that this task is a good proxy for a more general form of attacker behavior. While it bears a superficial resemblance to a hacking task, there are other possible proxies that would have served equally as well. Jordan and Taylor (1998) characterized the sociology of hackers and described some of the motivations of why they did the things they did. For some there is an element of game play. There is also a desire for a reward for what appears to be little effort. There is also a desire to rebel against the system.

Our proxy task included these points. The reward was higher than the prevailing wage on campus and the task didn't appear to be too difficult. Results of the experiment anecdotally showed that some did engage the test as a game and wanted to know the mechanism afterwards so they could judge their strategy. Finally, just calling it a hacking task, which was part of the initial briefing for participants, apparently did appeal to the rebellious nature as, again anecdotally, several of the participants commented on various counter culture themes as they accomplished the task.

This task also had the advantage in that it was objective and easy to administer fairly. Other tasks that were considered (i.e., a hacking simulation) would have been less straightforward and much more difficult to reduce statistically.

### 3.5 Initial Steps

This chapter describes the experimental methodologies used in this project. Over all, we conducted three separate experiments using procedures outlined here. These experiments have the approval by the University of Idaho's Institutional Review Board (see Appendix B).

Before the actual experiment began, several pilot groups of students were run over the summer to calibrate the variables of the experiment and the reward. This was also the beta test and allowed time to debug the software so that when there were a significant number of students in the system, time and funds were not wasted with faulty software.

Some randomly drawn dummy data were also created to test analysis methods. Random data tends to generate a straight line. When the data is clustered, it is possible to see curves or sharp drop-offs in behaviors.

The experimental group for the first two experiments was made up largely from students from the technical majors. No one was turned away, but the preponderance of technical majors was significant. These majors included but were not limited to Computer Science, Computer Engineering, Electrical Engineering, and MIS. The participants for the third experiment were volunteers from the students in the University of Idaho Commons during a two day period in December of 2012.

Each experimental group contained, as the literature suggests (Grossklags 2007), between four and twelve subjects in each trial. When gathering data in the Commons, only six stations were set up to limit the number in each trial. When private groups were solicited and a classroom or lab was used, the number of participants was limited to 12.



Participants were not allowed to be in more than one experiment. A sign in sheet was kept. No one attempted more than one experiment, but had it happened, the most recent experiment would have been disallowed. In accordance with IRB rules, the roster was destroyed after all testing was complete.

### **3.6 Experiment 1**

As stated in Section 1.4.1 the null hypothesis for this series of experiments is that there no relationship between the attack rate and the effectiveness of the security for a given level of return. In order to examine that relationship, Experiment 1 has been designed to measure how long a participant will stay with a task at a given reward level and then manipulate the security level. If there is no relationship, the totals would be similar at all reward levels for the attack rate. If the totals change, then how they change is the relationship in question.

Students were recruited to attempt to complete the security task which was to guess a password. An effort was made to get a reasonably large proportion of engineering and business students by appealing to them in their respective classes, but others were also selected. For Experiment 1, there was a modest monetary reward of \$0.50 per successful guessing of a password.

This amount was chosen because, as is shown in the cost analysis on the following page, the average student should make about \$10.00 for an hour of testing. This is the hourly wage of students with technical jobs on the University of Idaho campus and according to Grossklags (2007) matching the prevailing hourly wage for the student population is sufficient to motivate most students for the purposes of economic experiments. A wage which exceeds minimum wage attracts students with technical experience. Actual

experience showed that students made a little more than ten dollars an hour which was helpful in recruiting additional participants.

The difficulty of the task was varied by expanding the length of the password and the number of letters in the alphabet. This experiment is based on the work of Jonsson and Olovsson (1997) in their attempt to quantify the response of the single system attacker and Carbone and Geus (2004) with their work on digital data collection for Honey Pots.

Each student was given the security task of guessing a password from a restricted alphabet to access a secure site. The length of the alphabet and the length of the password were known to the subject. The numbers of attempts and the successes or failures were logged at each level.

The test had a limit of ten rounds. Each round was limited to ten minutes or ten successful guesses, whichever came first. The number of possible passwords was increased after each round. The participants could attempt each level of test as many times as they wished inside the ten minute limit for the round up to ten times. After each successful guess, the password was changed. The participant was not required to complete any specific level of test to be paid what he or she was owed.

The following survey data was also collected for each of the three experiments from each test participant to document the demographics of the test subjects without revealing personal identity.

1. Age
2. Gender
3. Major

4. Computer self-efficacy and relevant work and class experience. (see Appendix I)

The primary goal of the survey was to determine if there were any subgroupings in the sampled participants. Each section also had goals. The goal for Section 1 was to establish demographic data about the subjects.

Section 2 had two goals, to see if the participants had significant combinatorial math skills and to see if they had a mature view of problem solving. Determining their computer security knowledge was a definite plus.

The goal for Section 3 was to determine the participants' computer security self-efficacy. The instrument to measure computer self-efficacy was adapted from Rhee, Kim and Ryu (2009). Only the relevant portions of their instrument were used, those which focused on computer self-efficacy; portions dealing with control were not included. A copy of the survey is included in Appendix A. A seven-point Likert scale was used. The anchors of the scale were as follows:

1= Strongly Agree

2= Agree

3= Somewhat Agree

4= Neither Agree nor Disagree

5= Somewhat Disagree

6= Disagree

7= Strongly Disagree

In the first experiment, the participant could attempt the task as given or be given a less difficult task. The participant was given a cash reward for each success. Once the limit of this trial was reached, either in time or number of successes, the difficulty was increased and the process restarted. The levels of complexity are defined in Table 1. These levels were chosen to reduce the variability in the change of difficulty between complexity levels.

Limited pilot tests with prototype software suggested that starting with a two letter password and an alphabet of three possible letters enables each trial to be run in about ten seconds. If it is assumed that the password chosen is totally random, it can also be assumed that finding the correct password will, on average, take approximately half the time it would take to try all possible combinations. Table 1 shows the length of time and the projected cost for each subject.

Number of Letters in Alphabet	Number of Letters in Password	Possible Number of Passwords	Increase in Complexity	Estimated Time to Completion in Seconds	Estimated Completion	Estimated Payment	Estimated Wage per Hour	Estimated Time to End of Trial in Minutes
2	2	4		40	10.00	\$5.00	\$45.00	6.67
2	3	8	4	80	7.50	\$3.75	\$22.50	10.00
2	4	16	8	160	3.75	\$1.88	\$11.25	10.00
5	2	25	9	250	2.40	\$1.20	\$7.20	10.00
3	3	27	2	270	2.22	\$1.11	\$6.67	10.00
2	5	32	5	320	1.88	\$0.94	\$5.63	10.00
6	2	36	4	360	1.67	\$0.83	\$5.00	10.00
7	2	49	13	490	1.22	\$0.61	\$3.67	10.00
							\$15.32	76.67

**Table 1. Initial Payment Rates**

Note that password complexity was manipulated (size of password, length of password) to keep the change from one level to another relatively constant. Pilot testing on a limited number of participants (5) was completed to fine tune these figures.

At some point, if the participant declined to make further attacks because it became economically unattractive, his or her participation in the experiment would end. Each participant was paid in cash for the number of successfully completed tasks. The following metrics were captured for each participant:

1. Number of attempts required for each successful attack
2. Number of successful attacks and complexity level for each
3. Number of attempts at which the subject decided not to continue for the given complexity
4. Payment

Limited pilot testing showed that making scratch paper available would make the participant more likely to continue with testing as it made the security task easier to organize. In additional pilot tests we found that learning how to actively use scratch paper in this environment caused a dip in the number of attempts while participants figured out how to use it. The end result was that they stayed at the experiment longer but there was no other effect so scratch paper was not allowed in the full experiment.

### **3.7 Experiment 2**

Information from Experiment 1 was used to select the starting alphabet size and password length for Experiment 2 so that time and money was not wasted testing the participants in regions of alphabet size and password length that were not interesting. Results from the first experiment indicate that a password of length two and an alphabet of length eight is optimum.

For Experiment 2, the task was modified to test sensitivity to reward level. Reward level was started at \$1.00. The complexity of the hacking problem was held constant and

each time the task was completed, the reward was reduced by \$0.05 until the participant either exited the experiment or the reward went to zero. After each successful guess, the password was changed. The participant was not required to complete any specific level of test to be paid what he or she was owed.

The same metrics as described in Experiment 1 were captured for Experiment 2 as a basis for comparison.

### **3.8 Experiment 3**

For Experiment 3, methodology in Experiment 2 was followed but the reward level started at \$1.50 and was then reduced by \$0.05 for each success to see if it could generate a curve similar to the results of Experiment 1 but perhaps offset in some way. In the previous groups, a concerted effort was made to get business and engineering majors. For this experiment, everyone was accepted and there was advertising for business and engineering majors.

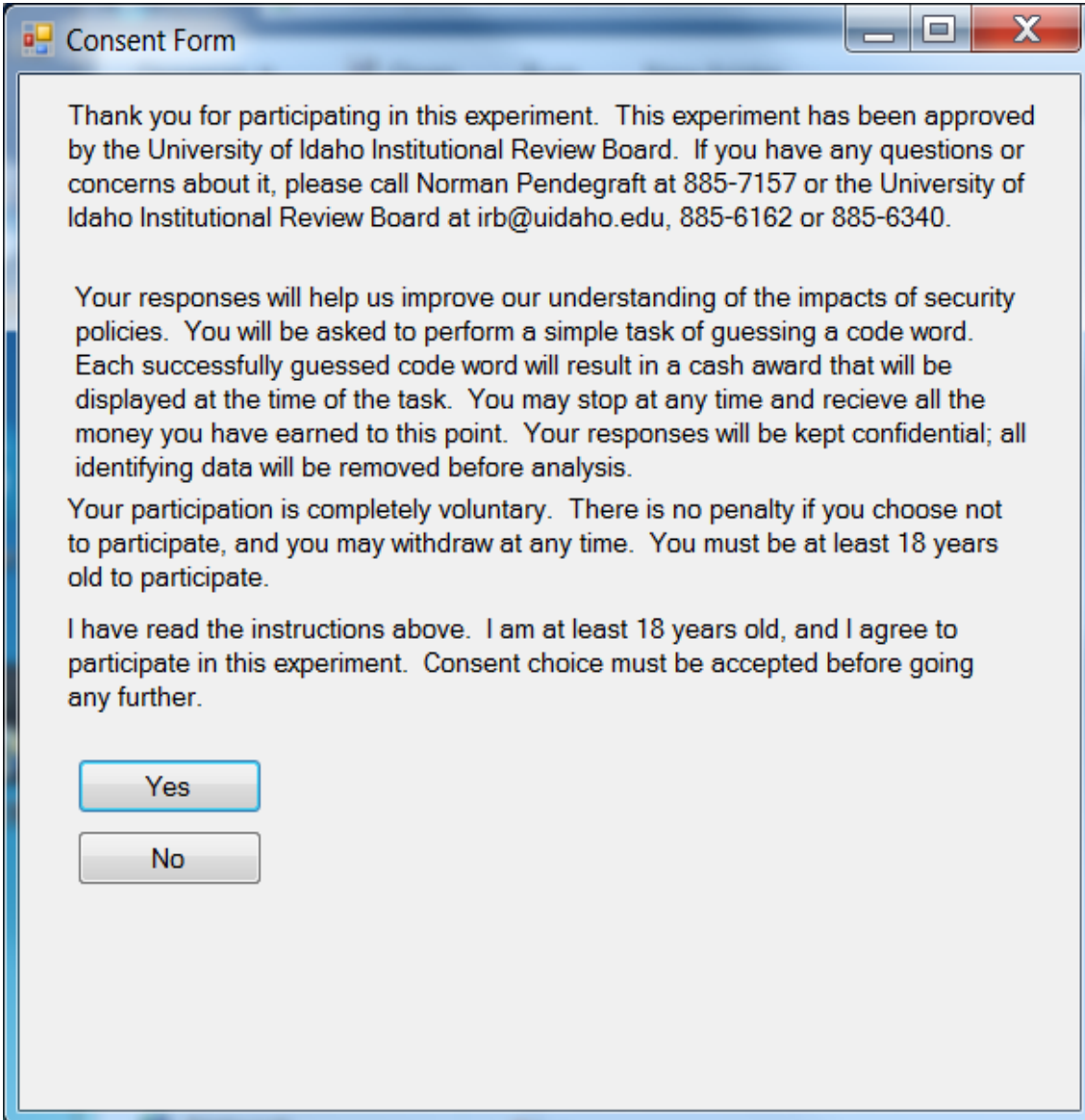
### **3.9 Software Framework**

The software for this project was developed with Visual Studios 2008 in Visual Basic. All data were stored using Access and linked via a common link to a virtual hard drive. An initial attempt was made to develop a website on which to run this experiment. The result was not stable in terms of data reporting, nor was it secure enough for purposes of the Intuition Review Board.

The second attempt used a virtual hard drive that was accessible in a controlled environment. Only one participant's data was completely lost, though there were several operator errors that lost portions of participants' records.

### 3.9.1 Consent Screen

The initial page of the software shows the consent form plus contact information for the researchers and the IRB as depicted in Figure 17.



Consent Form

Thank you for participating in this experiment. This experiment has been approved by the University of Idaho Institutional Review Board. If you have any questions or concerns about it, please call Norman Pendegraft at 885-7157 or the University of Idaho Institutional Review Board at irb@uidaho.edu, 885-6162 or 885-6340.

Your responses will help us improve our understanding of the impacts of security policies. You will be asked to perform a simple task of guessing a code word. Each successfully guessed code word will result in a cash award that will be displayed at the time of the task. You may stop at any time and receive all the money you have earned to this point. Your responses will be kept confidential; all identifying data will be removed before analysis.

Your participation is completely voluntary. There is no penalty if you choose not to participate, and you may withdraw at any time. You must be at least 18 years old to participate.

I have read the instructions above. I am at least 18 years old, and I agree to participate in this experiment. Consent choice must be accepted before going any further.

Yes

No

Figure 17. Consent Screen

Selecting “No” recorded that a participant refused and no other data were stored as per the instructions of the IRB. Selecting “Yes” opened the next window and began the experiment.

### 3.9.2 Demographics Screen

The software has three major sections. The first section gathered demographic information, some history of classes taken, possible computer experience, and assigned a participant number. At no time were data that could identify an individual stored or requested. This was to remain within the boundaries of the guidelines set by the Institutional Review Board. The demographic data were saved to an Access database with only the participant number. This screen is depicted in Figure 18.

The screenshot shows a software window titled "Demographics Quiz". The interface includes the following elements:

- A dropdown menu for "Please enter in your major:".
- A "Year In School" section with radio buttons for Freshman (selected), Sophomore, Junior, Senior, Graduate Student, and Other.
- A "Gender?" section with radio buttons for Male and Female.
- A text input field for "What is your age?".
- A question: "Have you ever held a position where one of your major responsibilities was configuring computer systems or networks?" with radio buttons for Yes and No.
- A text input field for "If the answer to the previous question is yes, what was your job title to the best of your knowledge?".
- A section titled "Please place a check next to any of the courses below that you have passed?" with a list of courses and checkboxes:
  - Math 310 Ordinary Differential Equations
  - Math 385 Theory of Computation
  - Math 386 Theory of Numbers
  - Math 476 Combinatorics
  - Math 578 Combinatorial Optimization
  - Any Senior or Graduate Level Math Class
  - CS 336 Introduction to Information Assurance
  - CS 385 Theory of Computation
  - Any Senior or Graduate Level Computer Science Course
  - Bus 355 Systems Analysis and Design
  - Bus 452 Business Telecommunications Management
- A "Next" button.

**Figure 18. Demographics Screen**



### 3.9.3 Computer Self Efficacy Quiz Screen

The second section ran the Computer Self Efficacy quiz to determine the score and saved the result via the participant number. The focus was not what they knew, but what they believed they knew. This was a proxy for confidence. This screen is depicted in figure 19.

Form3

Rate the following questions using this scale:

- 7 = Strongly Agree
- 6 = Agree
- 5 = Somewhat Agree
- 4 = Neither Agree nor Disagree
- 3 = Somewhat Disagree
- 2 = Disagree
- 1 = Strongly Disagree

I feel confident handling virus infected files.

I feel confident getting rid of spyware.

I feel confident understanding terms/words relating to information security.

I feel confident learning new methods to protect my information and information system.

I feel confident managing files in my computer.

I feel confident setting the Web browser to different security levels.

I feel confident using different programs to protect my information and information system.

I feel confident learning advanced skills to protect my information and information system.

I feel confident getting help for problems related to my information security.

I feel confident using the user's guide when help is needed to protect my information and information system.

I feel confident updating security patches to the operating system

Begin the experiment

Figure 19. Computer Efficacy Quiz

### 3.9.4 The Test

The final section ran the test. In all the experiments, the tests were run and the data kept on the local machine until the test was complete. This kept partial data from being entered into the database when computers crashed, when participants exited in an uncontrolled manner, or when the system was otherwise taken off the net. This screen is depicted in Figure 20.

The screenshot shows a window titled "Password Test Bed" with a standard Windows title bar. The main content area is titled "Instructions" and contains the following text:

Enter in a code selected from the potential alphabet displayed below. Letters may be used more than once. Press "Check Result" to check to see if you are correct. If you are correct, the system will initiate another test. If you wish to stop, press the stop button and your payment will be calculated and recorded.

Below the instructions, there is a table of parameters and a form for user input:

Alphabet	Alphabet Size	8	Participant Number	50
EOGPHDLA	Number of Possible Passwords	64		
Attempt	Code Word Length	2		
<input type="text"/>	Current Payment	0		
<input type="button" value="Check Result"/>	Payment Rate	\$1.50		

At the bottom center of the window, there is a "Stop" button.

**Figure 20. The Experiment**

This screen displayed the alphabet to choose from, plus numeric readouts about the size of the alphabet, the number of possible passwords, the current length, current payment,

payment rate, and the participant number. This number was the only identifying piece of information stored.

To complete the test, the participant needed to enter in the number in the text box labeled Attempt. Case wasn't important since all attempts were forced to upper case. The "Check Result" button compared the attempt to the actual code word. If the attempt was correct, a new alphabet was selected, the success including the number of attempts was stored, a new code word was selected, and the payment rate was added to the current payment.

If the attempt did not match the code word, the failure was recorded and the attempt window was cleared for a further attempt, assuming time or number had not expired for this round or the maximum number of successes (10) was not reached.

For the first experiment, if the attempt was correct, a counter was incremented. If this counter reached ten correct attempts, then the complexity was increased by either increasing the size of the alphabet or the code word. If not, then the alphabet was changed and a new code word of the same length chosen.

In the second and third experiments, when the attempt was correct, the payment rate was added to the current payment, the payment rate was decremented by \$0.05, and the code word and alphabet changed. Code word length remained the same. All the same data were recorded. Participants were allowed to continue to a payment rate of \$0.00 at which time they received an error message and the test was terminated. During the test, some participants wished to continue as they viewed it more as a game than something done for monetary reward.

## Chapter 4. Results

### 4.1 Analysis of Observations

This chapter statistically analyzes the observations from the experiments described in Chapter 3 and also looks at the various hypotheses to see if they are supported or rejected by these results.

#### 4.1.1 Research Question

In order to properly allocate scarce personnel, funds, and equipment, computer scientists need a better understanding of how hackers respond to security measures and how to model this behavior in complex information systems. Much information used in decision making is subjective. To move this line of inquiry from an art to a science the knowledge of attackers' responses must be quantified.

#### 4.1.2 Hypothesis

A focus of this research is based on system value and how attackers respond to changes in rewards based on that value. The first set of hypotheses asks the question "is whether there is a relationship between the attack rate and the complexity of the hacking task and what its shape is?" A more difficult hacking task should mean that people will need to be paid more to do it. As a reminder, the follow are the hypotheses.

(1<sup>st</sup> H<sub>0</sub>) There is no relationship between the attack rate and the complexity of the password.

(1<sup>st</sup> H<sub>1</sub>) There is a relationship between the attack rate and the complexity of the password and the complexity of the password reward is "S" shaped.

Experiment 1 was designed to test this hypothesis. In this experiment, as described in earlier chapters, there is fixed reward and the difficulty of a simple hacking task (guessing a password) is increased.

The intent of this experiment is to validate previously cited security models that use the “S” shaped curve to examine the behavior of complex information systems. One way to support this assumption would be to take this experimental data and show statistically that it resembles an “S” shaped curve. One mathematical representation of an “S” shaped curve is the logistic equation. This equation is in the form of:

$$F(x) = \mathcal{H} / (1 + e^{(\alpha * (x - \beta))})$$

Where  $\mathcal{H}$  is the maximum value of the function which is sometimes described as carrying capacity,  $\alpha$  is a constant defining the change in slope, and  $\beta$  is the inflection point of an “S” shaped curve. To approximate  $\beta$ , one half of  $\mathcal{H}$  was used. In a few cases, some adjustments were made to  $\beta$  after the first attempt to fit for optimization. These were all very small changes.

$\mathcal{H}$  was set to the maximum observed value of the parameter being measured (Number of Participants, Attack Rate, or Number of Successes) to approximate carrying capacity,  $\beta$  was set to one half of  $\mathcal{H}$ , approximating where the inflection point should be, and  $\alpha$  was varied by the goal seek tool. The goal was set to minimize the distance from the projected line of the logistic curve to the actual data.

$R^2$  values were used to judge the goodness of fit for each curve, and the F test was used to help determine the likelihood that this curve is represented by a logistic equation.

The test criteria based on the hypotheses is restated thusly:

$H_0$  is equivalent to F statistic < Critical Value

$H_1$  is equivalent to F statistic > Critical Value

In this case, the critical value varies with the number of categories being examined; the more categories the lower the F statistic needs to be. To interpret the data, a low F statistic (i.e. lower than the critical value) suggests that the similarity of the actual data vs. the logistic curve is not significant. This is the statement of status quo. A high F value means that the similarity between the logistic curve and the experimental data is significant, thereby rejecting  $H_0$ .

The critical value will vary based on the analysis being performed. In the F test, degrees of freedom equate to the number of categories of data being examined.

If these experiments reject the second null hypothesis which describes the notion that there is a curve that resembles a logistic function, it also rejects the first null hypothesis

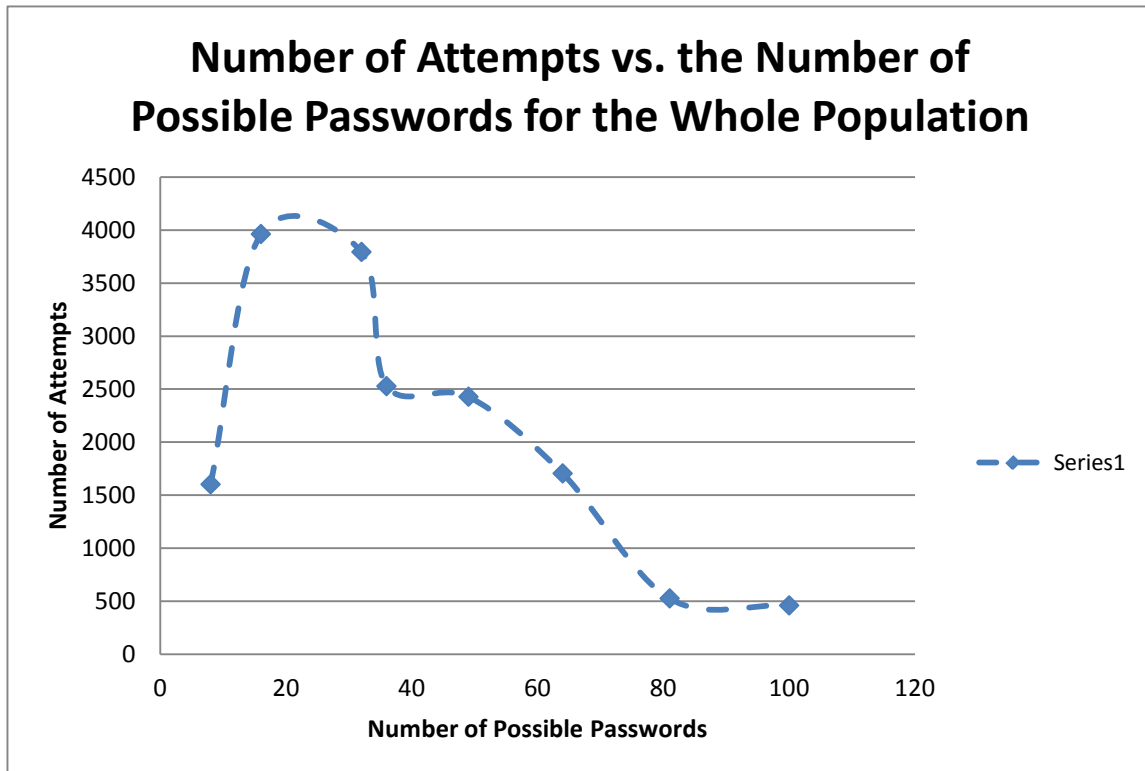
#### **4.1.3 Analysis of Experiment 1**

For Experiment 1, 63 individuals were tested, 52 of which were useful. One of the participants attempted to “hack” the system, terminating the experiment for that individual. In hindsight, it might have been better to record the results and mark it as an attempt to hack. Six data records had to be restarted when the participants inadvertently exited the program and as a result generated two records each, so the first in each case was deleted. Four records

were damaged where the experiments were correctly completed, but due to information transfer issues data was lost.

The graph of the 52 useful participants described in the paragraph above comparing the attack rate they made to the number of possible passwords is shown in Figure 21. There appears to be an “S” shaped curve after accounting for experimental artifacts. In this case, it is the fact that successes were limited to ten per trial. For lower levels of complexity this means that there will be fewer attempts. We statistically analyzed the goodness of fit for the curve in Table 2.

Following that are the three graphs (Figures 21, 22, and 23) that apply to the same data set as shown in Figure 20. For each graph, the actual data is shown with a solid line and squares for the data points and the generated logistic equation is shown with a dashed line and diamonds for the data points. The independent variable which varies for the purposes of this experiment is the complexity of the password. The number of attempts, the number of successes and the number participants were tested as dependent variables.



**Figure 21. Experiment 1, Total Number of Attempts vs. Number of Passwords Possible**

Figure 21 focuses on the number of attempts versus the number of possible passwords and shows what appears to be an “S” shaped curve.

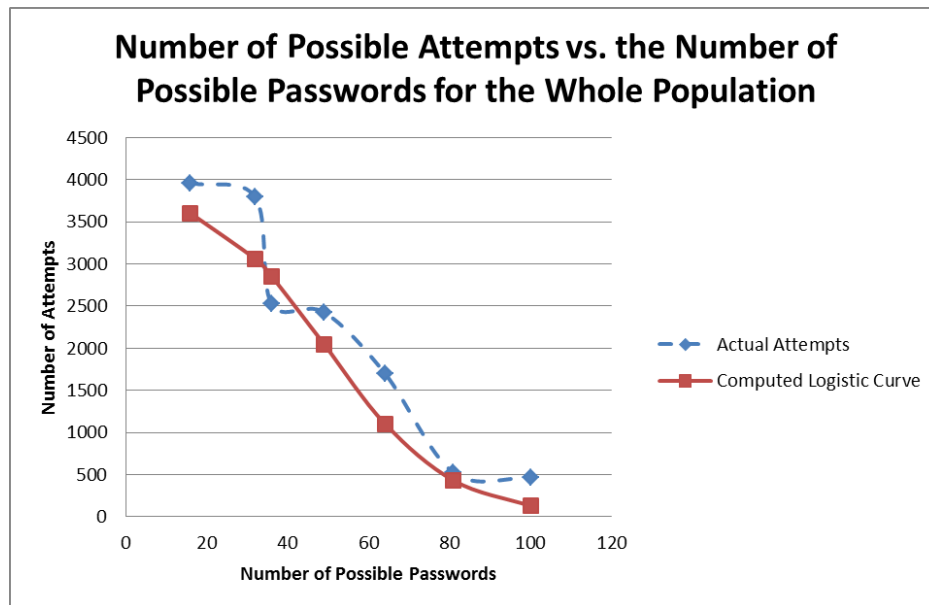
The number of attempts in Figure 21 for the first password is artificially low, because the number of successes was limited to ten. Because the password was simple, most participants completed all ten and as the complexity was not great, the number of attempts needed was low. Anecdotal evidence from participants as the complexity increased confirmed that they would have made many more attempts at that complexity level had the experiment been structured to allow that. Because of these issues and the fact that the budget was limited, this first data point was removed from consideration.

There seems to be a precipitous drop in attempts when the complexity exceeds 36 possible passwords. The number of attempts exceeds the schedule in Table 1 (which only



went as high as 49) because a portion of the participants continued past the point where Grossklags (2007) said they would stop. Based on anecdotal conversations with those who remained, it appears they did so because they viewed the Experiment as something akin to a computer game or logic puzzle and were playing it for fun at this point.

When that first data point was removed, the result was the following graph in Figure 22:



**Figure 22. Experiment 1, Number of Attempts vs. Number of Passwords Possible**

The next graph (Figure 23) shows the number of participants versus the number of possible passwords. It also supports the notion of an “S” shaped curve. Charting the number of participants at each increase in complexity shows that, until complexity reaches thirty six possible passwords, there is little dropout. Then the drop is significant. It levels out when only a few focused individuals are left.

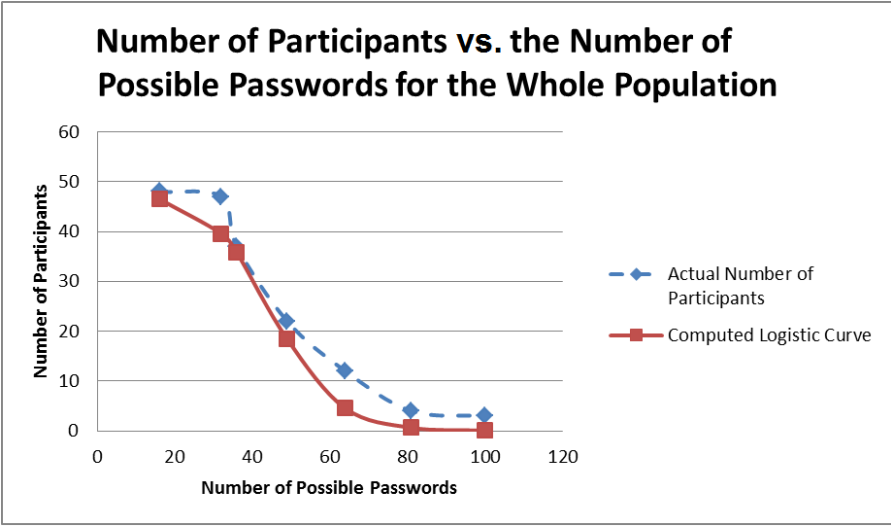


Figure 23. Experiment 1, Number of Participants at Each Level vs. Number of Passwords Possible

Figure 24 shows the number of successes versus complexity. The drop is significant almost from the beginning. It levels out when only a few focused individuals are remaining.

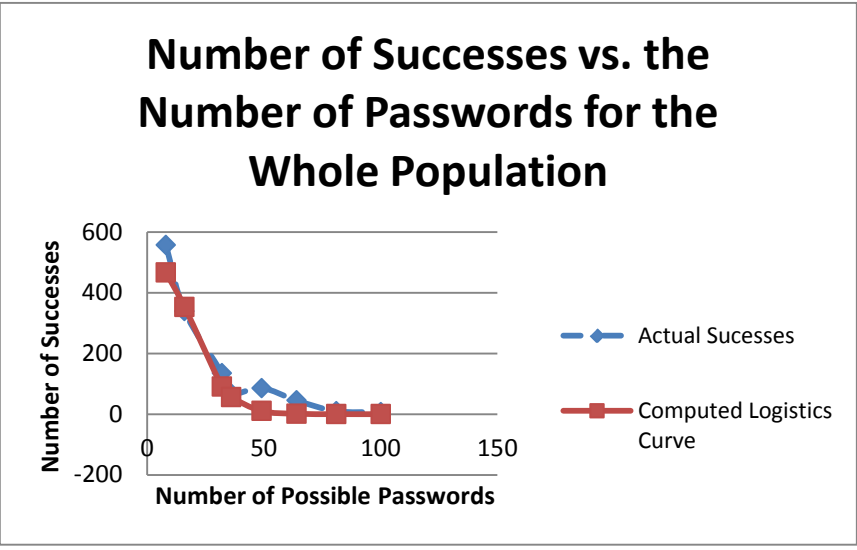


Figure 24. Experiment 1, Number of Successes at Each Level vs. Number of Passwords Possible

Table 2 shows the logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, the critical value for making that determination and the reasons why the critical value changes for the whole data set. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis. For this experiment, the critical value varies. The reason is that the number of categories range from four to eight. The more categories, the lower the critical value is.

Experiment One							
All Participants							
Measure	Best Fit	$R^2$	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Reason for Change in the Critical Value	Null Rejected
Attempts	$y = 3962 / (1 + e^{(-.068 * (x - 50))})$	0.9689	213.34	4.28 = $F_{6,6}(.05)$	8.47 = $F_{6,6}(.01)$	Dropped one node	Yes
Participants	$y = 48 / (1 + e^{(-.119 * (x - 45))})$	0.9916	748.72	4.28 = $F_{6,6}(.05)$	8.47 = $F_{6,6}(.01)$	Dropped one node	Yes
Successes	$y = 557 / (1 + e^{(-.137 * (x - 20))})$	0.9832	317.01	3.78 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Uses all the data nodes	Yes

**Table 2. Experiment 1, Complete Data Set**

This data shows strong support for the “S” shaped curve in these analyses as the F values are two orders of magnitude higher than the critical values at this level of confidence. For attempts and participants,

#### 4.1.4 Clustering

Visual inspection backed up with cluster analysis shows that there are two major groups in the data. Referring to Figures 24 and 25, there is a clear stair step when the complexity as defined by the number of possible passwords reached 36. The first group is the participants with the highest level of attempts and successes, all of whom got to the 49 password level before they decided to quit. They had the highest level of attempts and success. The second group is the lower portion containing 30 participants. Based on this, the data was clustered into two groups. The first is all of the data, the first cluster (called the top cluster) and then the second cluster (called the bottom cluster). To show this more clearly, the clusters have been circled in Figure 25.

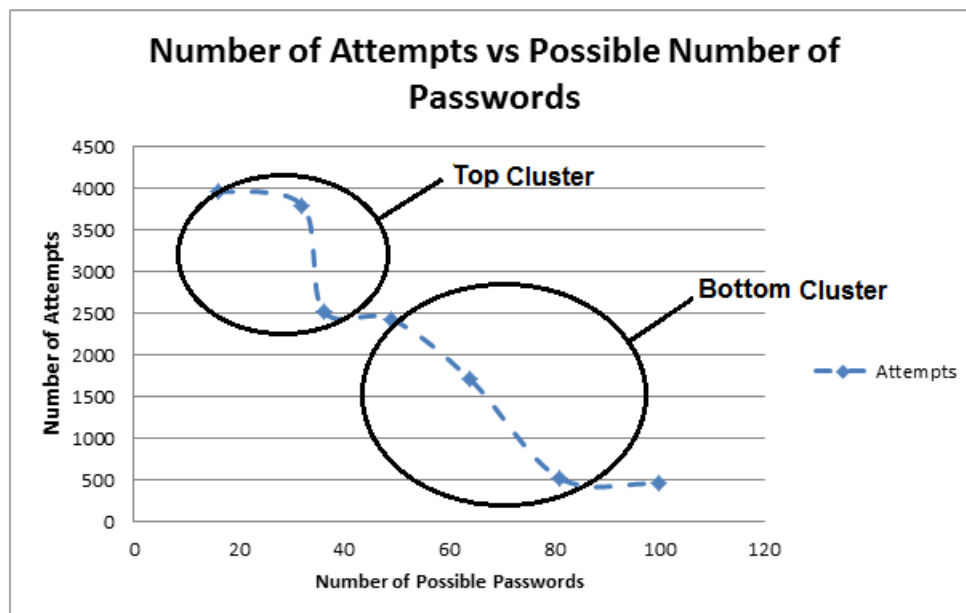
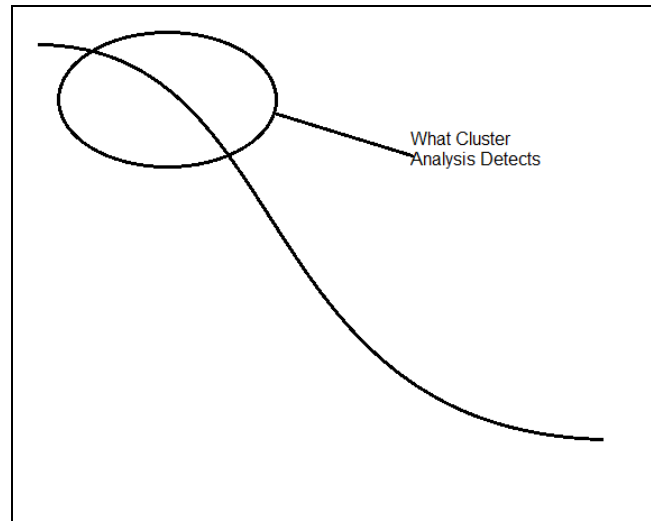


Figure 25. Experiment 1, Number of Attempts vs. Number of Passwords Possible with Cluster Circled



**Figure 26. What Cluster Analysis Captures**

K means cluster analysis was used to confirm this visual interpretation. K values of two, three and four used and clusters that remained stable were selected. Cluster analysis finds only a portion of the “S” shaped curve. Figure 26 shows that cluster analysis very good at picking out the steep drop-off or the “knuckle” that is characteristic of an “S” shaped curve. To actually see the curve, the outliers of the group that is represented in the cluster analysis must also be included. In this case, it was all of the participants who got to (though didn’t always complete) the 49 possible password level.

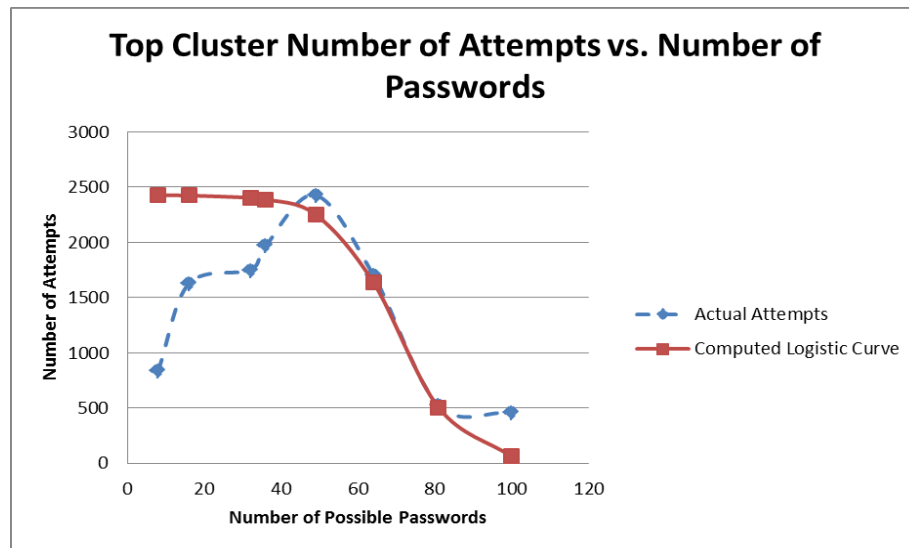
Based on this, the data was divided into two groups for analysis. These clusters are referred to as the Top and Bottom clusters.

When K (the constant defining the number of clusters) was equal to four and five, there were three clusters that remained constant; when K was equal to three; two of those clusters, the two with the highest average attempts were still the same as before. All clustering was Euclidian in nature and all three measures; attempts, successes and the number of participants at any given level were used to define the clusters.

#### 4.1.5 The Top Cluster

The first group is the participants with the highest total number of attempts and successes, all of whom reached at least 49 possible password level before they decided to quit. This group tended to show an “S” shaped curve which is backed up by the results of the R2 goodness of fit test and the hypothesis testing using the F statistic to compare the logistic curve and that experimental result.

The next three graphs show this top cluster and compare the number of attempts (Figure 27), the number of participants (Figure 28), and the number of successes (Figure 29) versus the number of possible passwords as described in the previous section for the whole population.

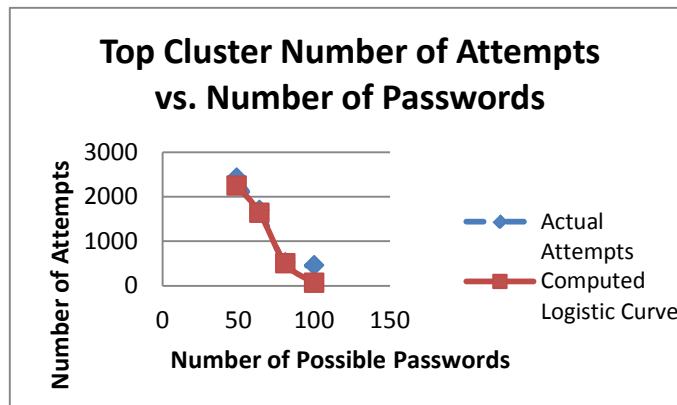


**Figure 27. Experiment 1, Number of Attempts vs. Number of Passwords Possible for the Top Cluster**

In Figure 27, the initial start step previous to the “S” shaped decline is an artifact of the experiment since each participant was limited to ten successes at each level. This subgroup had the maximum number of successes and the reduced number of attempts is because less complex passwords require fewer attempts on average to guess the correct one.

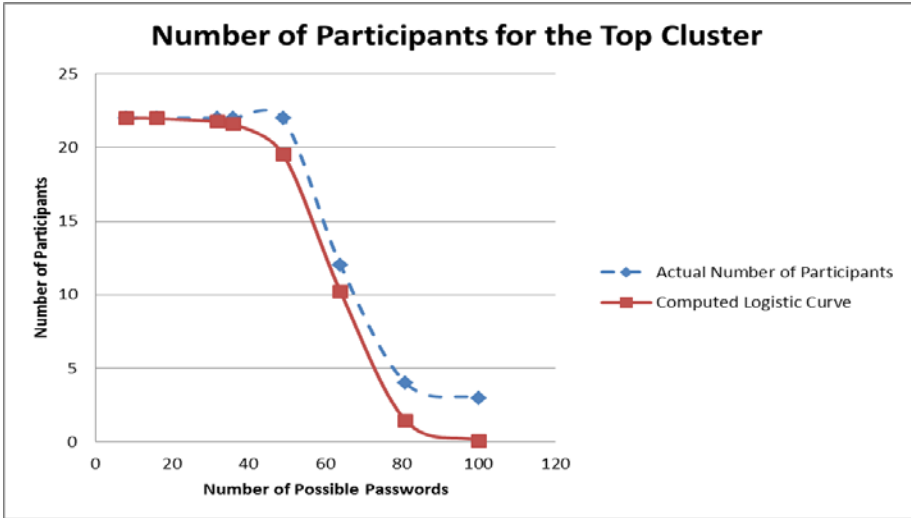
This group contained all the participants who played all the way to the end of the experiment.

Taking the four data points that occur after they stop maxing out the successes generates a graph shown in Figure 28.



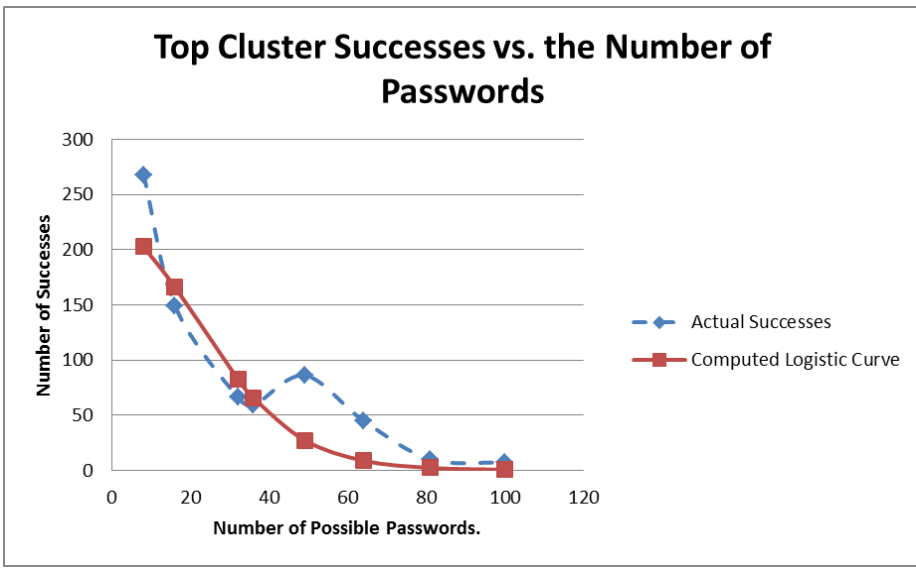
**Figure 28. Experiment 1, Number of Attempts vs. the Number of Passwords Possible for the Top Cluster for the Last Four Data Points**

Figure 29 shows the number of participants at each level. As expected, this shows a potential “S” shaped curve with a few dedicated participants holding on until the end. Three of these participants, when they were asked to stop, made clear the fact that they would have continued even without the reward as they found the game stimulating.



**Figure 29. Experiment 1, Number of Participants vs. Number of Passwords Possible at Each Level for the Top Cluster**

When observing the successes in Figure 30 the curve appears to be a more straight forward “S” shaped curve. The decline is much more marked and steady. The low  $\beta$  value which denotes the inflection point which occurs when the number of possible passwords reaches eighteen or nineteen suggests that there will be less of an initial shelf than seen in previous graphs. The actual graph bears this out.



**Figure 30. Experiment 1, Number of Successes vs. the Number of Passwords Possible at Each Level for the Top Cluster**



Table 3 is arranged in the same manner as Table 2 with logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, the critical value for making that determination and the reasons why the critical value changes for the whole data set. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis and again data shows strong support for the “S” shaped curve in these analyses as the F values are very high, though the Successes are only a single magnitude higher than the critical value which rejects the null hypothesis in each case.

Experiment One							
Top Cluster							
Measure	Best Fit	$R^2$	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Reason for Change in Critical Value	Null Hypothesis Rejected
Attempts	$y = 2428/(1+e^{-.122*(x-70)})$	0.9866	147.29	9.27 = $F_{3,3}(.05)$	29.5 = $F_{3,3}(.01)$	Limited due to Maxing the test	Yes
Participants	$y = 22/(1+e^{-.148*(x-63)})$	0.9965	573.38	3.78 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Uses all the data nodes	Yes
Successes	$y = 268/(1+e^{-.081*(x-22)})$	0.924	24.84	3.78 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Uses all the data nodes	Yes

Table 3. Experiment 1, Top Cluster

#### 4.1.6 The Bottom Cluster

The next three graphs (Figures 31-34) show the bottom cluster’s results that compare the number of attempts, the number of participants, and the number of successes versus the number of possible passwords. The first, Figure 31, shows the number of attempts. As has been seen before, the first data point is an artifact of the experiment because the number of successes was limited to ten. The drop is definitive as these participants almost uniformly quit when the number of possible passwords increased beyond 36 for most of them and 49 for the most intense.

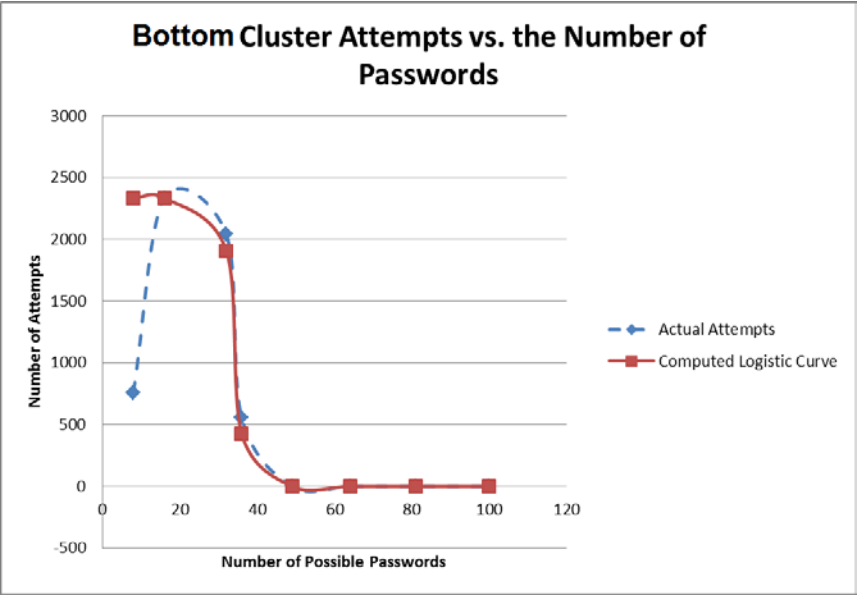


Figure 31. Experiment 1, Number of Attempts vs. Number of Passwords Possible at Each Level for the Bottom Cluster

The next graph (Figure 32) shows the number of participants at each level. What made this cluster interesting is the marked difference in behavior. All of these participants stopped when the number of possible passwords exceeded 36.

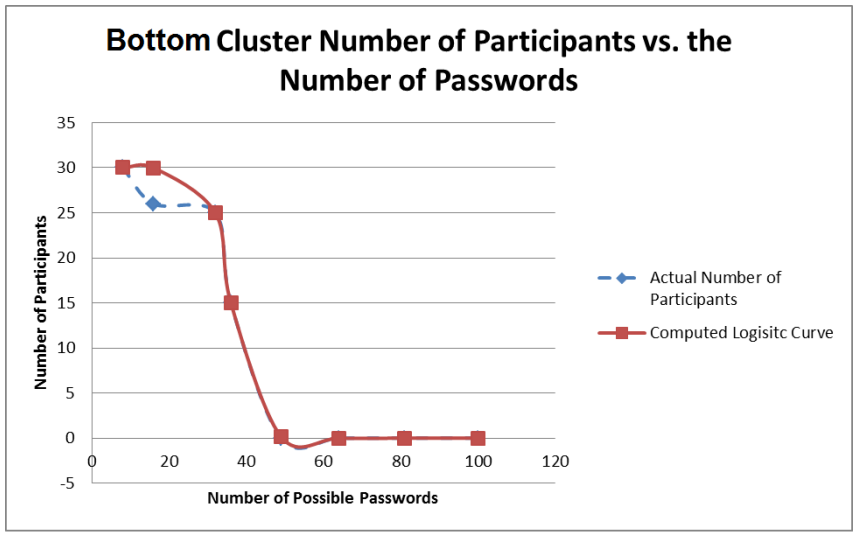
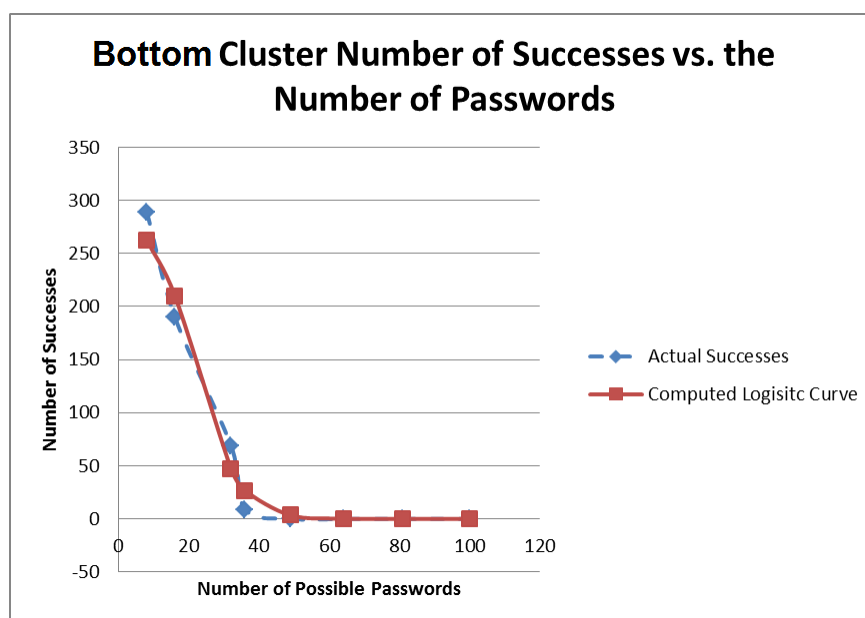


Figure 32. Experiment 1, Number of Participants vs. Number of Passwords Possible at Each Level for the Bottom Cluster

The last graph, Figure 33, in this sequence shows the number of successes. This drops aggressively as these participants appear to have a lower motivation.



**Figure 33. Experiment 1, Successes vs. Number of Passwords Possible at Each Level for the Bottom Cluster**

Table 4 is arranged in the same manner as Table 2 and 3 with logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, the critical value for making that determination and the reasons why the critical value changes for the whole data set. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis and again data shows strong support for the “S” shaped curve in these analyses as the F values are the highest yet, with the value for successes being three orders of magnitude higher than needed which rejects the null hypotheses and supports the theory that these response curves are in fact “S” shaped.

Experiment One						
Bottom Cluster						
Measure	Equation	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 2334/(1+e^{-.751*(x-34)})$	0.9559	1582.65	9.27 = F <sub>3,3</sub> (.05)	29.5 = F <sub>3,3</sub> (.01)	Yes
Participants	$y = 30/(1+e^{-.401*(x-36)})$	0.9958	650.45	9.27 = F <sub>3,3</sub> (.05)	29.5 = F <sub>3,3</sub> (.01)	Yes
Successes	$y = 289/(1+e^{-.163*(x-22)})$	0.9894	272.10	9.27 = F <sub>3,3</sub> (.05)	29.5 = F <sub>3,3</sub> (.01)	Yes

Table 4. Experiment 1, Bottom Cluster

## 4.2 Analysis of Experiment 2

### 4.2.1 Hypothesis for Experiment 2

A focus of this research is based on system value and how attackers respond to changes in rewards based on that value. The hypotheses ask the question is there a relationship between the attack rate and the size of the reward and what is its shape? In this experiment, the difficulty of the hacking task remains the same, and reward starts at \$1.00 and decreases by \$0.05 each time a participant successfully guesses a password. At some point, they will determine that it is no longer worth the effort and stop. There is no limit to the number of attempts.

(1<sup>st</sup> H<sub>0</sub>) There is no relationship between the attack rate and the size of the reward.

(1<sup>st</sup> H<sub>1</sub>) There is a relationship between the attack rate and the size of the reward and that relationship is “S” shaped..

Experiments 2 and 3 tested these hypotheses as discussed in Experiment 1. The logistic equation is a mathematical representation of an “S” shaped curve. These equations are in the form:

$$F(x) = \mathcal{H}(1 + e^{(\alpha * (x - \beta))})$$

The average number of attempts is probably the best measure of motivation because it is a measure of the actual effort put into the completing the security task. The number of attempts was compared between experiments to determine if there was a difference in the level of motivation or desire to complete the task. A hypothesis to describe this comparison follows:

$H_0$  = The average number of attempts for Experiment 1 equals the average number of attempts for Experiment 2.

$H_1$  = The average number of attempts for Experiment 1 is less than the average number of attempts for Experiment 2.

Using the Student t distribution (Encyclopædia Britannica, 2014), the t obtained is calculated with the following formula:

$$t_{obtained} = \frac{\bar{x} - \mu}{\hat{s} / \sqrt{N}}$$

where  $\bar{x}$  is the sample of interest, in this case, the average number of attempts for Experiment 2's participants.  $\mu$  is the mean that is tested against, in this case, the average number of attempts for Experiment 1's participants.  $\hat{S}$  is the standard deviation of the sample in question which in this case is Experiment 2. N is the number in the sample, in this case 48. The critical value is determined using the degrees of freedom which are N-1 and the level of confidence required which in most research is 95%. This is a one-tailed test as only the figures greater than the mean are relevant. Using these figures, the critical value is 1.684.

#### **4.2.2 Analysis for Experiment 2**

For Experiment 2, 56 individuals were sampled, generating 54 useful results. Reasons for rejection included two attempts to "hack" the experiment, someone who had to be restarted and as a result generated two records, and two damaged records where the experiment was correctly completed but due to participant misunderstanding of instructions, data were lost. As with the attempted hack in Experiment 1, recording the data from the two that attempted to hack the system might have been useful.

In Experiment 2 it was found that the number of attempts people were willing to make is statistically higher than Experiment 1. In Experiment 1, the average number of attempts was 320.5 with a standard deviation of 239.6. Experiment 2 generated an average of 411.4 with a standard deviation of 247.9. The t obtained was 2.54. This rejects the null hypothesis and makes the case that the participants in Experiment 2 were more motivated than those in Experiment 1.

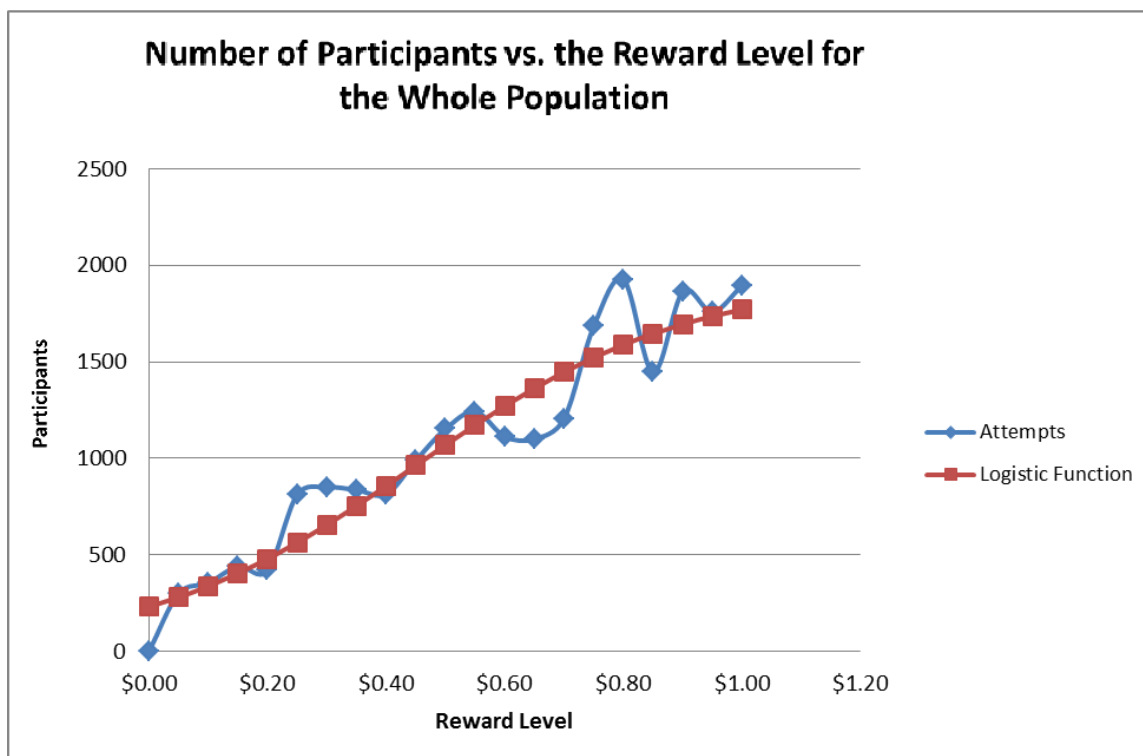
This result is interesting since it seems to indicate that if the task itself doesn't change, people are willing to make more attempts because they don't have to puzzle out a

new method. The statistically significant higher number of attempts for Experiment 2 supports the concept that defense should be layered with multiple defense mechanisms instead of crustal.

### 4.2.3 Graphical Analysis for Experiment 2

The number of attempts versus the reward level shows the most deviation from a logistic curve as shown in Figure 34. There seem to be three curves in this graph.

Later graphs (figures 35, 36, and 37) will also show these three curves. The greater variability in the number of attempts as compared to the number of successes and the number of participants that is apparent in this graph is interesting. It appears in all three subgroups' measure of attempts. There may be a learning curve issue here as most of the measures settle down as time goes on.



**Figure 34. Experiment 2, Number of Attempts vs. Reward Level for the Whole Population**

Figure 35 suggests that there are at least three levels. They have been circled to identify them more clearly.

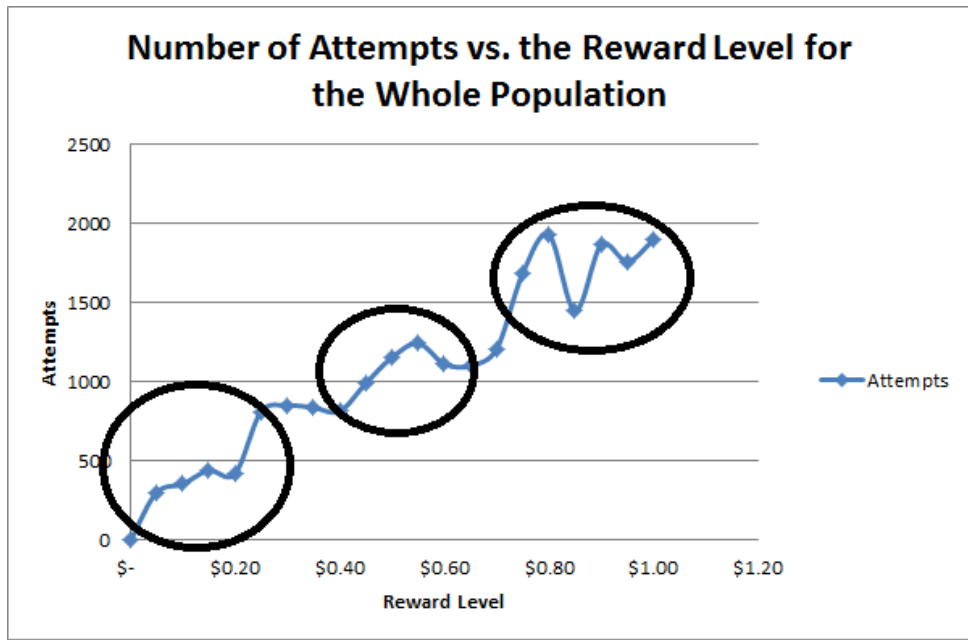


Figure 35. Experiment 2, Number of Attempts vs. Reward Level for the Whole Population Clusters Circled

Figure 36 shows the number of participants at each level of reward. Here again there are three levels. This graph shows the least level of variability.

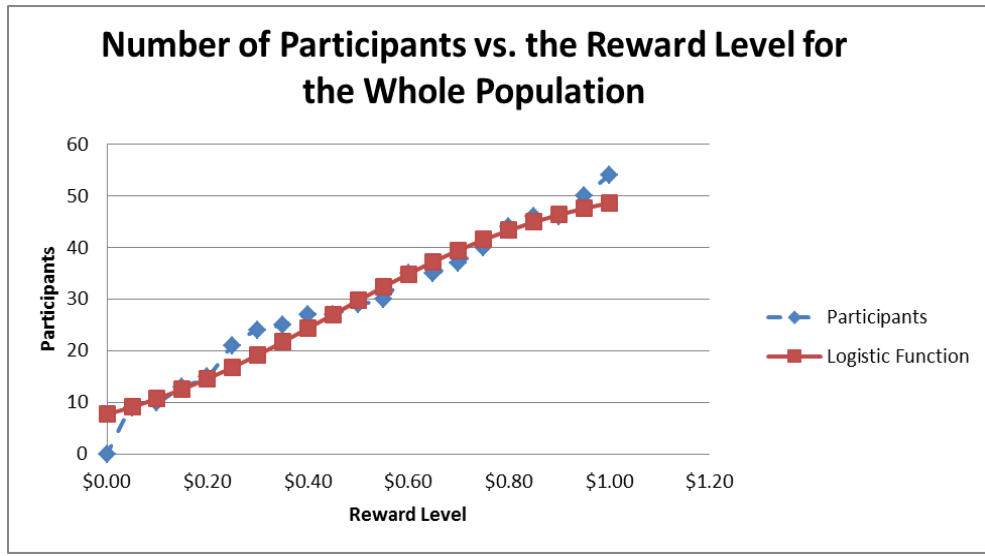


Figure 36. Experiment 2, Number of Participants vs. Reward Level for the Whole Population



The final graph in the section (Figure 37) is the number of successes at various reward levels. There were a number of individuals who failed to make a success in the allotted time and the still continued on with the next trial for less reward. This graph also shows three levels and is the closest to an “S” shaped curve.



**Figure 37. Experiment 2, Number of Successes vs. Reward Level for the Whole Population**

Table 5 shows the results for the computed logistic curve for each of the graphs. The critical value for all the graphs is the same, as experimental realities did not require the removal of specific data points.

Table 5 is arranged in the same manner as Table 2 with logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, and the critical value for making that determination. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis. The data shows support for the “S” shaped curve in these analyses as the F values are high, with Attempts scored the lowest at something over two times the amount required to reject the null hypothesis.

Experiment Two						
All Data						
Measure	Best Fit	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 1927/(1+e^{(4.42*(x-0.45)})})$	0.9837	5.038	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes
Participants	$y = 54/(1+e^{(3.99*(x-0.45)})})$	0.9845	15.88	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes
Successes	$y = 48/(1+e^{(4.32*(x-0.35)})})$	0.9832	16.61	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes

Table 5. Experiment 2, All Participants

Visual inspection backed up with cluster analysis shows that there are three major groups in the data. Referring to Figures 38 through 41, there is a clear stair step when the reward reaches \$0.35 and again when it reaches \$0.65. To show this more clearly, the clusters are circled in Figure 38.

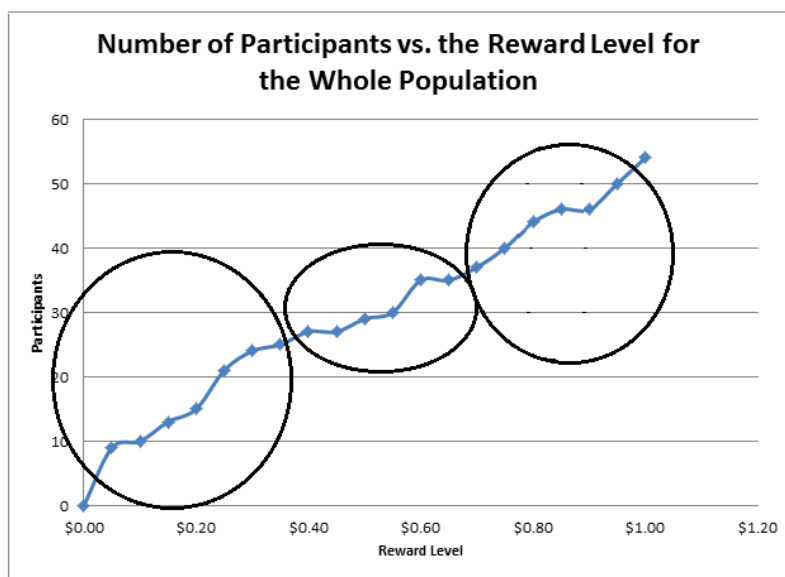


Figure 38. Experiment 2, Number of Participants vs. Reward Level Possible with Clusters Circled

K means cluster analysis was used to confirm this visual interpretation. There appear to be three clusters or knuckles on the graph of the number of participants vs. the reward

level for experiment 2 (Figure 39). Based on this, K means cluster analysis was run with  $K =$  to three, four, five, and six. When  $K$  was equal to four, five, and six, there were two clusters that kept the same data points, and when  $K$  was equal to three, one of those clusters, the one with the highest average attempts, still retained all the same data points. Based on this, the data was divided into three groups for analysis. These clusters are referred to as the Top, Center, and Bottom clusters.

#### 4.2.4 Graphical Analysis for Experiment 2 Top Cluster

Participants selected for the Top cluster all attempted 14 passwords and all but four were successful. For all of these failures, all but one decided to continue with the next attempt.

Figure 39 shows the number of attempts these participants generated during the test. While again, it is the most variable of the measures, it still shows something that might be interpreted as a visible “S” shaped curve. However this graph (Figure 40) did not come close enough to reject the null hypothesis.

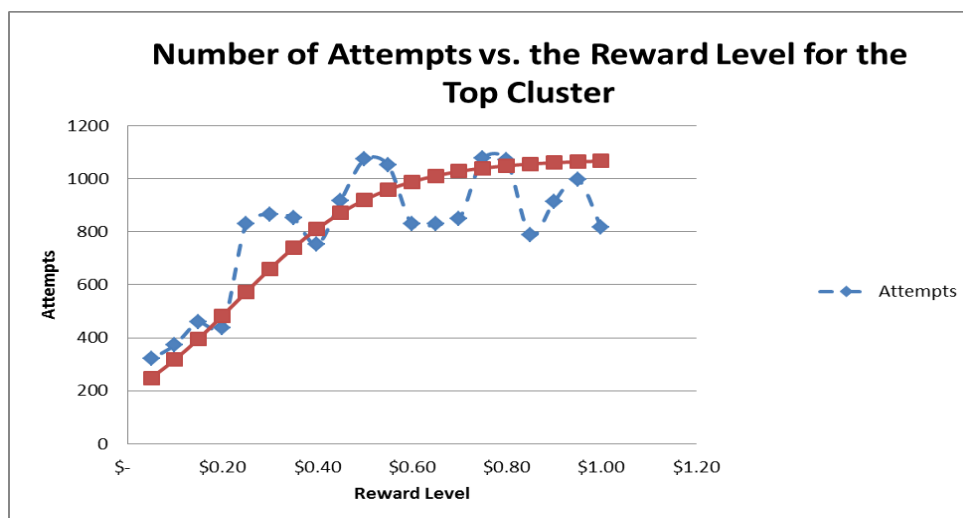


Figure 39. Experiment 2, Number of Attempts vs. Reward Level for the Top Cluster

The next graph (Figure 40) shows the number of these participants at each reward level. The “S” shaped curve here is much more pronounced than in the previous graph. Several would have continued on after the reward had expired had they not been stopped.

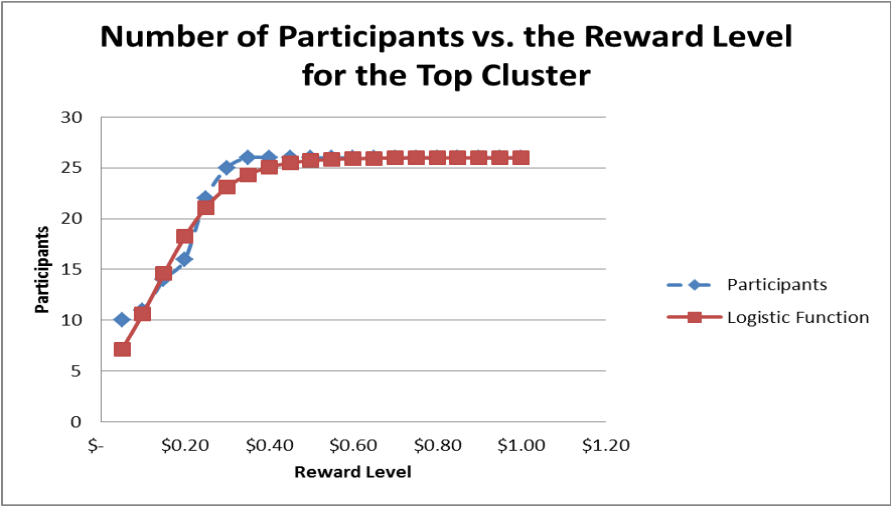


Figure 40. Experiment 2, Number of Participants vs. Reward Level for the Top Cluster

The final graph (Figure 41) for this cluster is that of the number of successes vs. each reward level. There appears to be an “S” shaped curve in this graph as well.

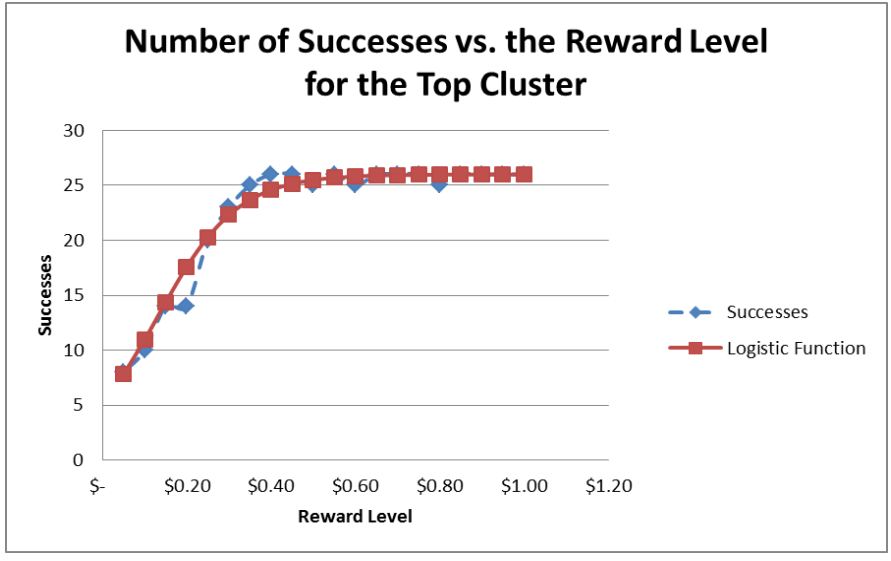


Figure 41. Experiment 2, Number of Successes vs. Reward Level for the Top Cluster

Table 6 is arranged in the same manner as Table 2 with logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, and the critical value for making that determination. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis. The data shows support for the “S” shaped curve in these analyses as the F values are high, actually higher than for the whole population. Attempts scored the lowest and did not actually reject the null hypothesis for this curve. The critical value for rejection of the null hypothesis remains the same as all of the reward levels are in play and the number of participants in this cluster exceeds 25.

<b>Experiment Two</b>						
<b>Top Cluster</b>						
Measure	Best Fit	$R^2$	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 1073/(1+e^{(6.65*(x-0.23)})})$	0.8403	1.316	2.12 = $F_{9,40}(.05)$	2.89 = $F_{9,40}(.01)$	No
Participants	$y = 26/(1+e^{(12.19*(x-0.13)})})$	0.9837	15.08	2.12 = $F_{9,40}(.05)$	2.89 = $F_{9,40}(.01)$	Yes
Successes	$y = 26/(1+e^{(10.57*(x-0.13)})})$	0.9854	16.97	2.12 = $F_{9,40}(.05)$	2.89 = $F_{9,40}(.01)$	Yes

**Table 6. Experiment 2, Top Cluster**

#### 4.2.5 Graphical Analysis for Experiment 2 Center Cluster

This cluster is somewhat problematical as it has only ten participants. Because of that and the fact that they did not carry through to the lowest reward level, the critical value for rejecting the null hypothesis is somewhat higher at 2.84.

The first graph (Figure 42) shows the number of attempts versus the reward level for this cluster. Again, attempts are too variable to reject the null hypothesis ( $\alpha=5\%$ ).

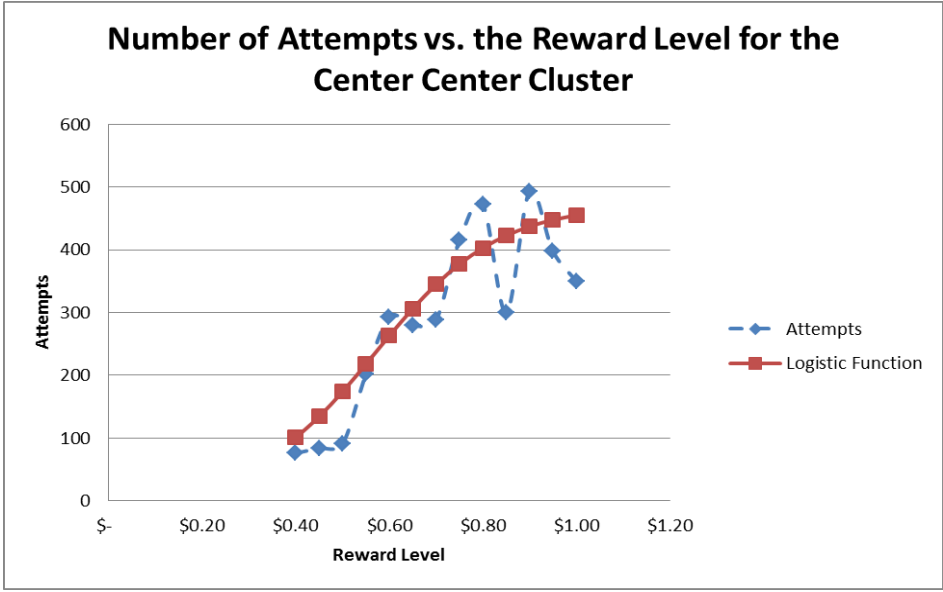


Figure 42. Experiment 2, Number of Attempts vs. Reward Level for the Center Cluster

Figure 43 shows the number of participants versus the reward level for this center cluster. The resemblance to an “S” shaped curve is notable and the results do reject the null hypothesis.

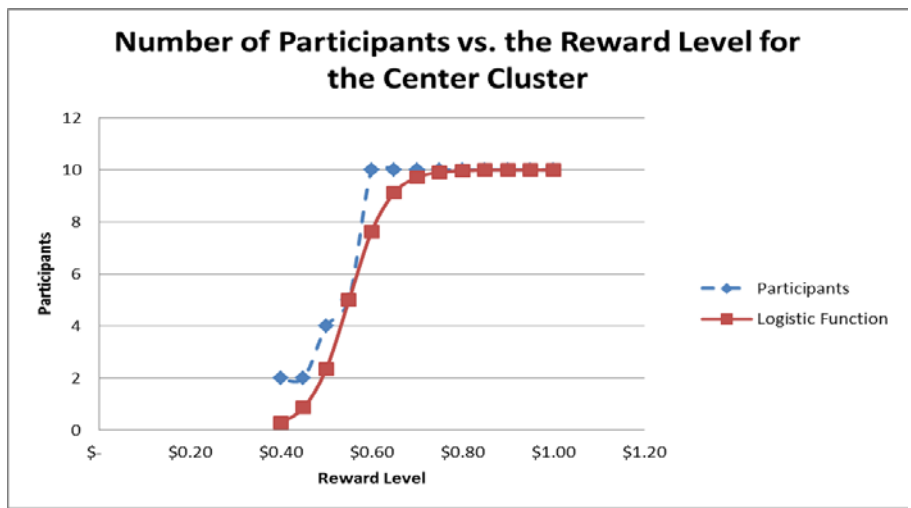


Figure 43. Experiment 2, Number of Participants vs. Reward Level for the Center Cluster

The number of Successes is also graphed in Figure 44. This also shows a significant resemblance to an “S” shaped curve. Statistical analysis on Table 7 shows that these results do reject the null hypothesis.

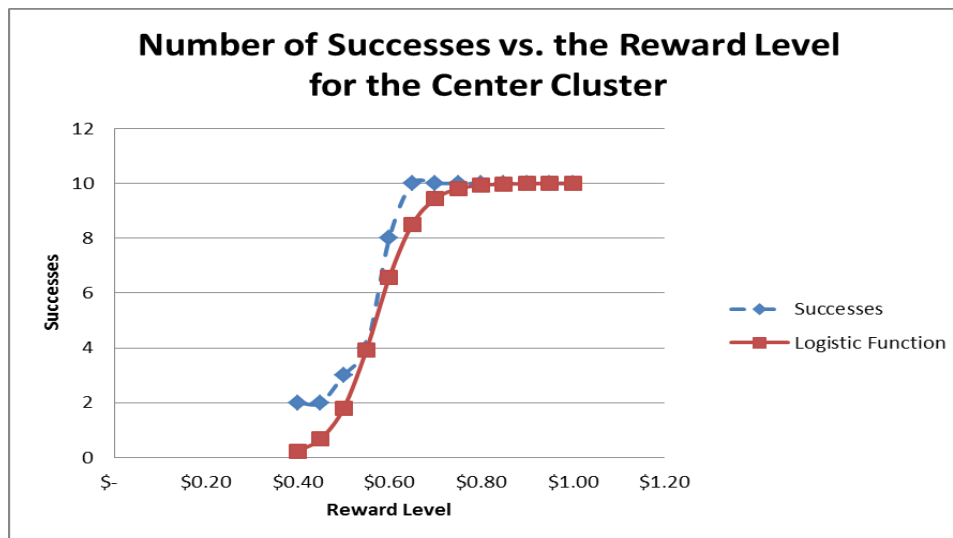


Figure 44. Experiment 2, Number of Successes vs. Reward Level for the Center Cluster

Table 7 is arranged in the same manner as Table 1. Attempts scored the lowest and did not actually reject the null hypothesis for this curve. The critical value for rejection of the null hypothesis is somewhat higher at 2.84.

Experiment Two						
Center Cluster						
Measurement	Bet Fit	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 472/(1+e^{(7.68*(x-0.57))})$	0.9004	1.893	2.84 = $F_{7,24}(.05)$	3.50 = $F_{7,24}(.01)$	No
Participants	$y = 10/(1+e^{(23.51*(x-0.55))})$	0.9813	10.51	2.84 = $F_{7,24}(.05)$	3.50 = $F_{7,24}(.01)$	Yes
Successes	$y = 10/(1+e^{(21.72*(x-0.57))})$	0.9894	18.79	2.84 = $F_{7,24}(.05)$	3.50 = $F_{7,24}(.01)$	Yes

Table 7. Experiment 2, Center Cluster

#### 4.2.6 Graphical Analysis for Experiment 2 Bottom Cluster

This cluster is larger at nineteen participants. Because of the fact that they did not carry through to the lowest reward level and in fact most quit quite early, the critical value for rejecting the null hypothesis is somewhat higher at 3.51.

The first graph (Figure 45) shows the number of Attempts versus the reward level for this cluster. In this cluster, Attempts reject the null hypothesis.

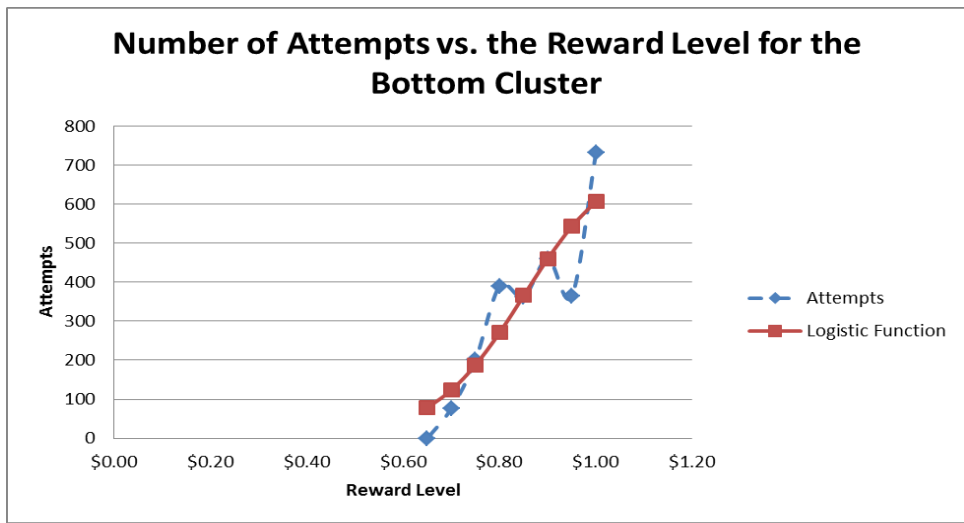


Figure 45. Experiment 2, Number of Attempts vs. Reward Level for the Bottom Cluster

Figure 46 shows the number of participants versus the reward level for the bottom cluster. The resemblance to an “S” shaped curve is notable and the results do reject the null hypothesis.

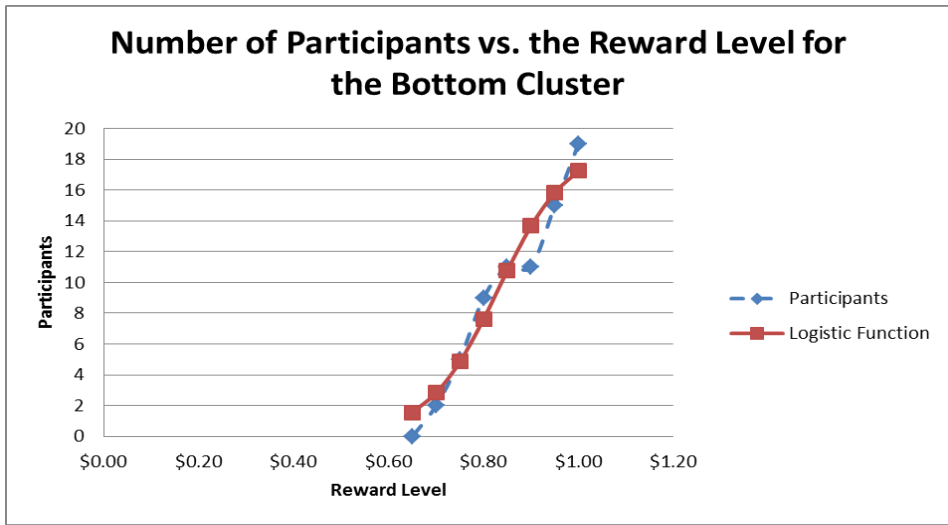
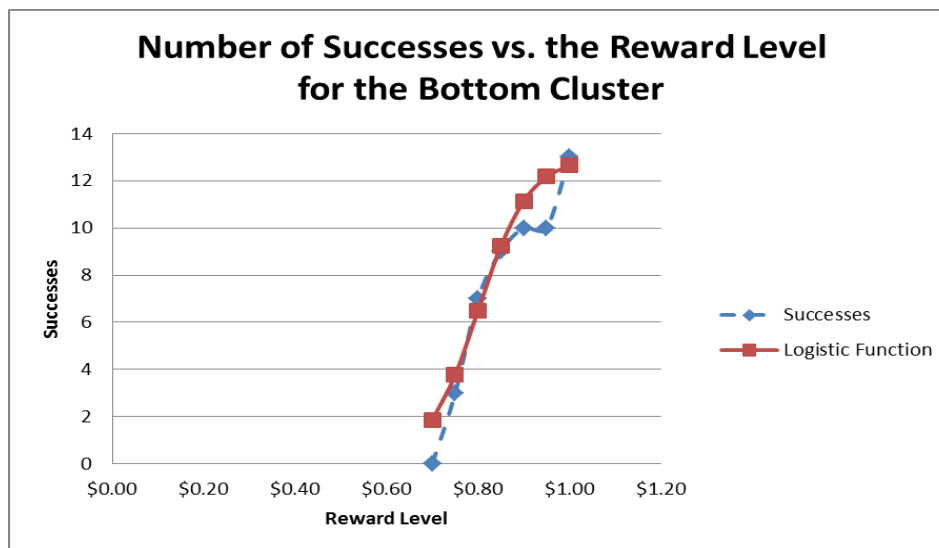


Figure 46. Experiment 2, Number of Participants vs. Reward Level for the Bottom Cluster



The number of Successes is graphed in Figure 47. This also shows a significant resemblance to an “S” shaped curve. Statistical analysis of Table 8 shows that these results do reject the null hypothesis.



**Figure 47. Experiment 2, Number of Successes vs. Reward Level for the Bottom Cluster**

Table 8 is arranged in the same manner as Table 1. The critical value for rejection of the null hypothesis is somewhat higher at 3.51 ( $\alpha=5\%$ ).

Experiment Two						
Bottom Cluster						
Measure	Equation	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 731/(1+e^{(10.605*(x-0.85)})})$	0.9036	11.73	3.51 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Yes
Participants	$y = 19/(1+e^{(13.42*(x-0.83)})})$	0.9742	47.27	3.51 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Yes
Successes	$y = 13/(1+e^{(17.9*(x-0.80)})})$	0.9736	46.22	3.51 = $F_{7,7}(.05)$	6.99 = $F_{7,7}(.01)$	Yes

**Table 8. Experiment 2, Bottom Cluster**

### 4.3 Analysis of Experiment 3

#### 4.3.1 Hypothesis for Experiment 3

Methodology for Experiment 3 is exactly the same as Experiment 2 except that instead of starting the payments at a dollar (\$1.00) payments were started at \$1.50. Fifty two individuals were sampled generating fifty useful results. Two individuals had to be restarted and as a result generated two additional records that had to be removed.

The average number of attempts made by each population was also tested as in Experiment 2 in an attempt to compare motivations between experiments. For this test, the hypotheses are as follows:

$H_0$  = The average number of attempts for Experiment 1 equals the average number of attempts for Experiment 2 and Experiment 3.

$H_1$  = The average number of attempts for Experiment 1 and 3 is less than the average number of attempts for Experiment 3.

Using the Student t distribution (Encyclopædia Britannica, 2014), the t obtained figure can be calculated with the following formula:

$$t_{obtained} = \frac{\bar{x} - \mu}{\hat{s} / \sqrt{N}}$$

where  $\bar{x}$  is the sample of interest, in this case, the average number of attempts for Experiment 2's participants.  $\mu$  is the mean tested against, in this case, the average number of attempts for Experiment 1's participants.  $\hat{S}$  is the standard deviation of the sample in question which in this case is Experiment 2. N is the number in the sample, in this case 48. The critical value is determined using the degrees of freedom which is N-1 and the level of confidence required which in most research is 95%. This is a one-tailed test as only the values greater than the mean are relevant. Using these values, the critical value is 2.0096.

In Experiment 3, the number of attempts people were willing to make is statistically higher than in Experiment 1 or 2. In Experiment 1, the average number of attempts was 320.5 with a standard deviation of 239.6. Experiment 2 generated an average of 411.4 with a standard deviation of 247.9. In Experiment 3, the average number of attempts was 500.1 with a standard deviation of 271.22. The t obtained when compared against Experiment 1 was 4.68 and when compared against Experiment 2 was 2.31. In this case, the critical value is 2.0096 so the null hypothesis can be rejected and the average for Experiment 3 is shown to be statistically higher than Experiments 1 and 2. This rejects the null hypothesis and makes the case that the participants in Experiment 3 were more motivated than those in Experiments 1 and 2.

#### **4.3.2 Graphical Analysis for Experiment 3**

The number of attempts versus the reward level shows the most deviation from a logistic curve as shown in Figure 48. There seem to be three curves in this graph.

A later graph (Figure 51) will also show these three areas in greater detail. The greater variability that is apparent in this graph is interesting. It appears in all three sub

groups. Other measures do not show this much variability. There may be a learning curve issue here as most of the variations in the measures decrease as time goes on.

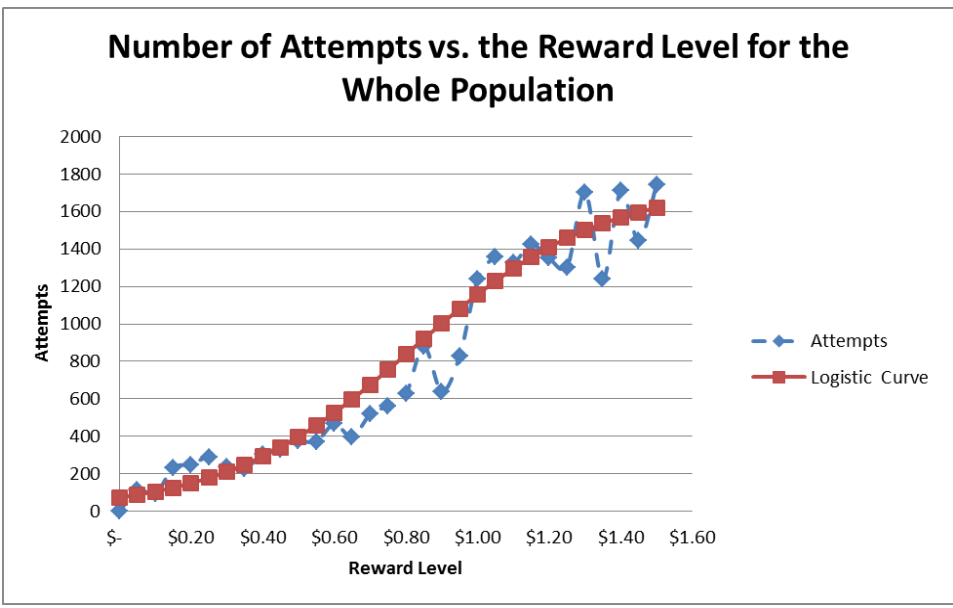


Figure 48. Experiment 3, Number of Attempts vs. Reward Level for the Whole Population

Figure 48 shows the number of participants at each level of reward. Here again there appear to be three levels. This graph shows the least level of variability. It also shows a resemblance to an “S” shaped curve.

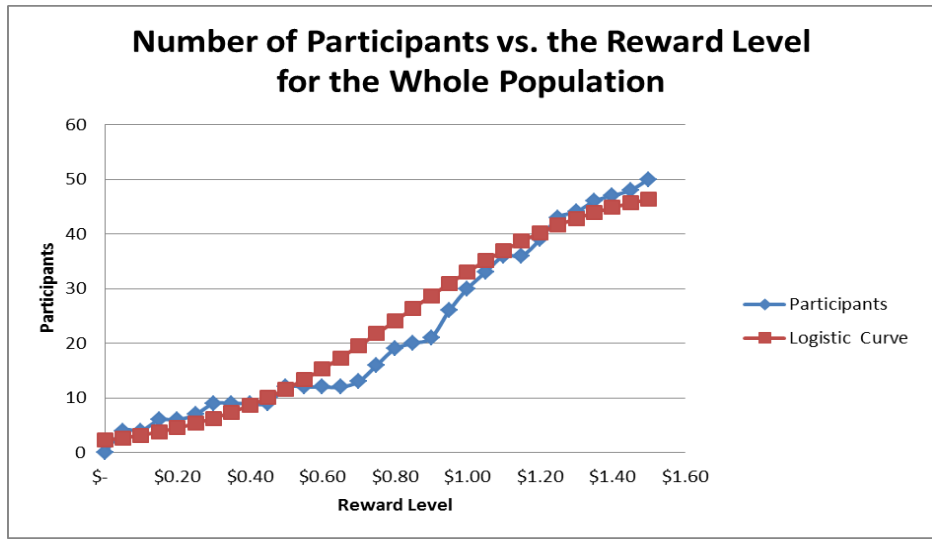


Figure 49. Experiment 3, Number of Participants vs. Reward Level for the Whole Population

The final graph in the section (Figure 50) is the number of successes at various reward levels. The data shows that a number of individuals would fail to make a success in the allotted time and still go on with the next trial for less reward. This graph also shows three levels and is the closest to an “S” shaped curve.



**Figure 50. Experiment 3, Number of Successes vs. Reward Level for the Whole Population**

Table 9 shows the results for the computed logistic curve for each of the graphs. The critical value for all the graphs is the same, as experimental realities and did not require the removal of specific data points.

Table 9 is arranged in the same manner as Table 1 with logistic equations,  $r^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, and the critical value for making that determination. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis and again data shows support for the “S” shaped curve in these analyses as the F values are high, all over 11; Attempts scored the lowest at over four times the amount required to reject the null hypothesis.

Experiment Three						
All Data						
Measure	Best Fit	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 1741/(1+e^{(3.81*(x-0.82))})$	0.9676	11.36	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes
Participants	$y = 50/(1+e^{(3.72*(x-0.82))})$	0.9790	17.79	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes
Successes	$y = 50/(1+e^{(3.72*(x-0.82))})$	0.9791	17.80	2.12 = F <sub>9,40</sub> (.05)	2.89 = F <sub>9,40</sub> (.01)	Yes

Table 9. Experiment 3, All Participants

Visual inspection backed up with cluster analysis shows that there are three major groups in the data. Referring to Figures 47 through 49, there is a clear stair step when the reward reaches thirty five cents and again when it reaches sixty five cents. To show this more clearly, the clusters are circled in Figure 51. Participants were used as the clustering criteria as this graph shows the least variability, but the three groups were apparent in all three.

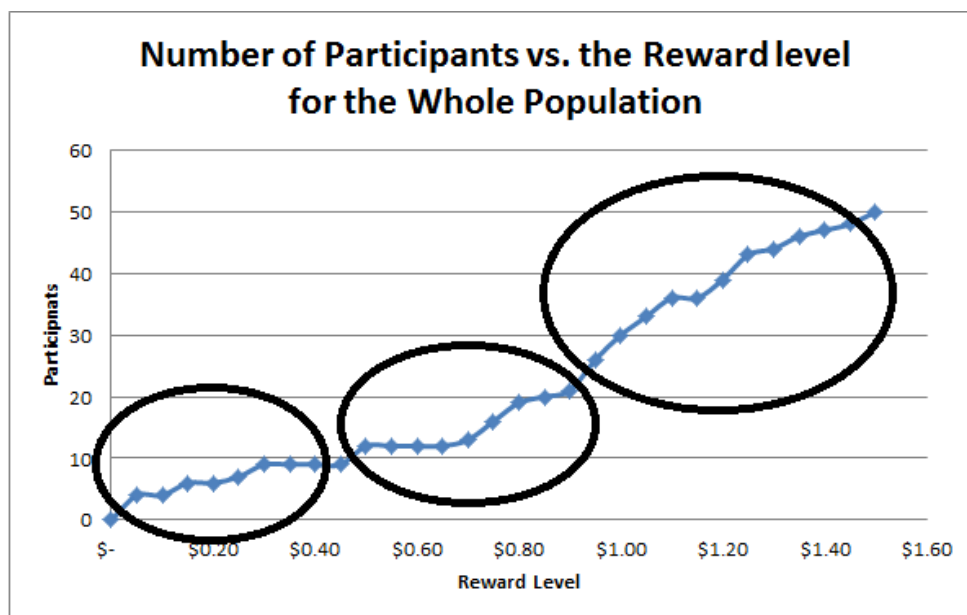
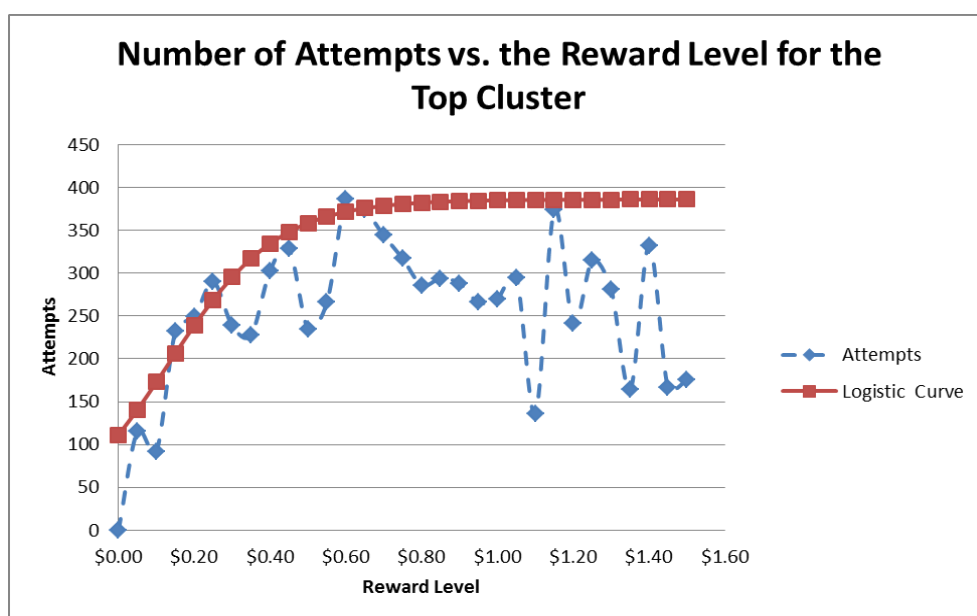


Figure 51. Experiment 3, Number of Participants vs. Reward level Possible with Clusters Circled

### 4.3.2 Graphical Analysis for Experiment 3 Top Cluster

This cluster is somewhat problematical, because as with Experiment 3, it has only ten participants. Participants selected for the Top cluster completed each trial until the reward reach \$0.35. At this point, they began to quit. Of the nine participants in this cluster, four continued on until the test terminated.

Figure 52 shows the number of attempts these participants generated during the test. While again, it is the most variable of the measures, it still shows something that might be interpreted as a visible “S” shaped curve. However this graph (Figure 48) did not come close enough to reject the null hypothesis.



**Figure 52. Experiment 3, Number of Attempts vs. Reward Level for the Top Cluster**

The next graph (Figure 53) shows the number of these participants at each reward level. The “S” shaped curve here is much more pronounced than in the previous graph. Several would have continued on after the reward had expired had they not been stopped.

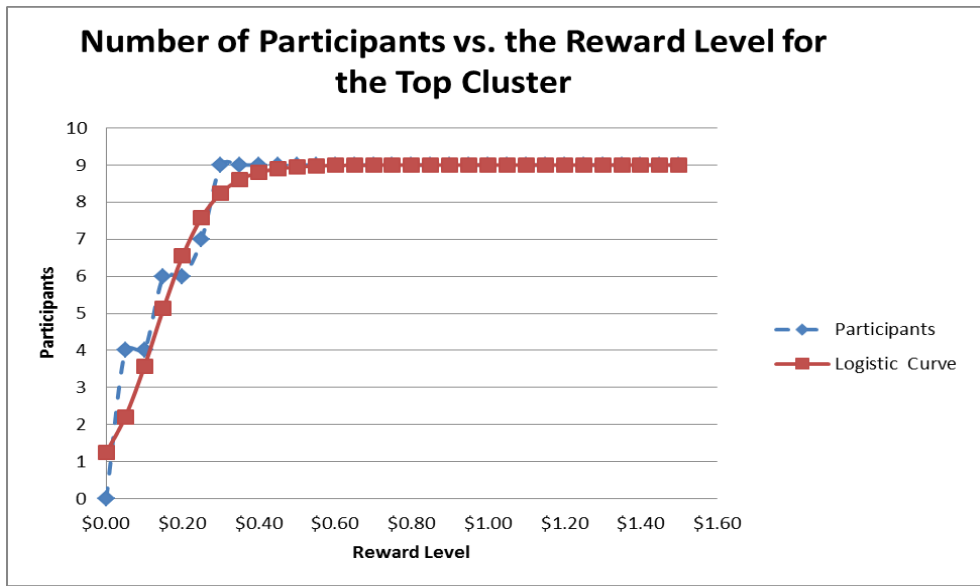


Figure 53. Experiment 3, Number of Participants vs. Reward Level for the Top Cluster

The final graph (Figure 54) for this cluster is that of the number of successes vs. each reward level. There appears to be an “S” shaped curve in this graph as well.



Figure 54. Experiment 3, Number of Successes vs. Reward Level for the Top Cluster

Table 10 is arranged in the same manner as Table 1 with logistic equations,  $R^2$  values for determining the goodness of fit, the F value which shows how likely the data is accurately mapped by the logistic equation, and the critical value for making that



determination. Finally, it contains a column that makes clear whether or not this analysis rejects the null hypothesis. The data shows support for the “S” shaped curve in these analyses as the F values are high, actually higher than for the whole population. Attempts scored the lowest and did not actually reject the null hypothesis for this curve. The critical value for rejection of the null hypothesis is higher as the number of participants is only 9 at 2.25 ( $\alpha=5\%$ ).

<b>Experiment Three</b>						
<b>Top Cluster</b>						
Measure	Equation	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 386/(1+e^{(6.94*(x-0.13)})})$	0.6287	1.316	2.25 = $F_{9,27}(.05)$	3.15 = $F_{9,27}(.01)$	No
Participants	$y = 9/(1+e^{(14.02*(x-0.13)})})$	0.9733	28.37	2.25 = $F_{9,27}(.05)$	3.15 = $F_{9,27}(.01)$	Yes
Successes	$y = 9/(1+e^{(11.65*(x-0.13)})})$	0.9763	32.07	2.25 = $F_{9,27}(.05)$	3.15 = $F_{9,27}(.01)$	Yes

**Table 10. Experiment 3, Top Cluster**

#### 4.3.3 Graphical Analysis for Experiment 3 Center Cluster

This cluster has seventeen participants. Because of the smaller cluster, the critical value for rejecting the null hypothesis is somewhat lower at 2.46. It did raise the value slightly because they did not continue through to the end.

The first graph (Figure 55) shows the number of attempts versus the reward level for this cluster. This curve has some resemblance to an “S” shaped curve and its F value is just barely high enough to reject the null hypothesis.

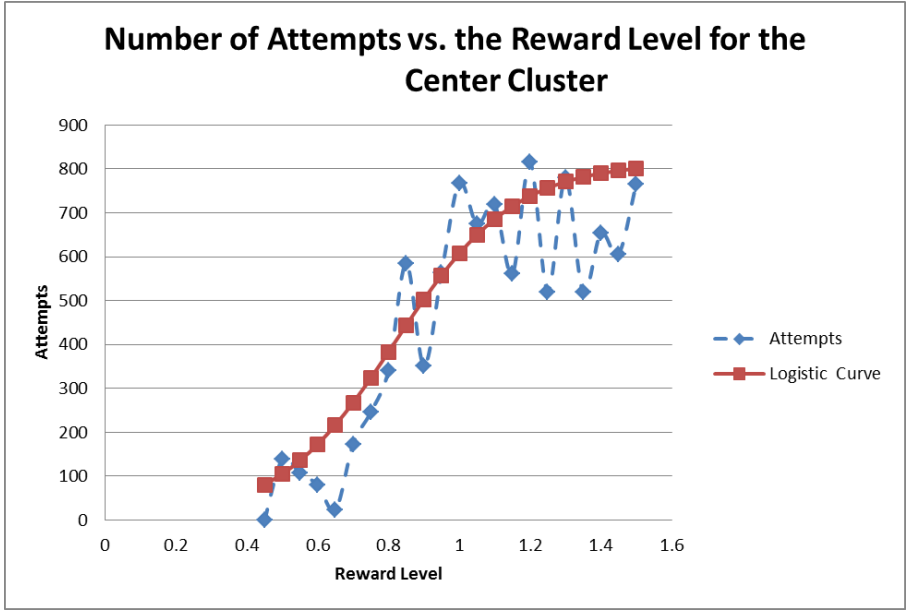


Figure 55. Experiment 3, Number of Attempts vs. Reward Level for the Center Cluster

Figure 56 shows the number of participants versus the reward level for this center cluster. The resemblance to an “S” shaped curve is notable and the results do reject the null hypothesis.

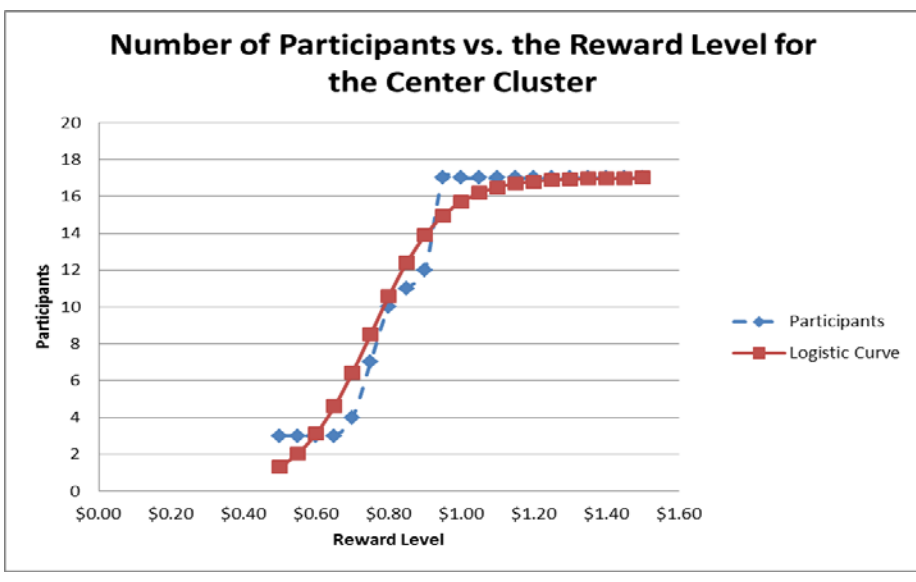
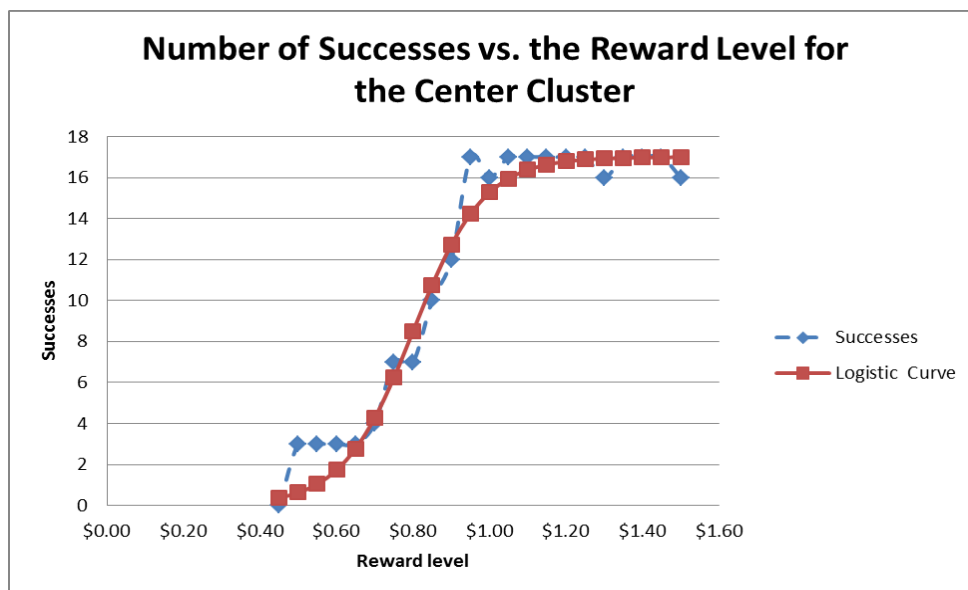


Figure 56. Experiment 3, Number of Participants vs. Reward Level for the Center Cluster

The number of successes are also graphed in Figure 57. This also shows a significant resemblance to an “S” shaped curve. Statistical analysis shows that these results do reject the null hypothesis ( $\alpha=5\%$ ).



**Figure 57. Experiment 3, Number of Successes vs. Reward Level for the Center Cluster**

Table 11 is arranged in the same manner as Table 1. Attempts scored the lowest and did not actually reject the null hypothesis for this curve. The critical value for rejection of the null hypothesis is somewhat lower at 2.46.

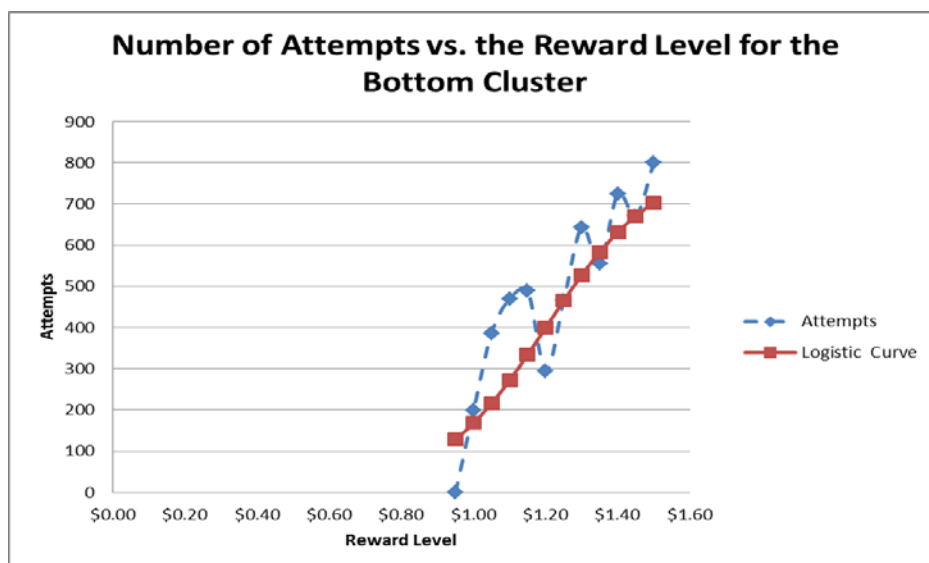
Experiment Three						
Center Cluster						
Measure	Equation	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 99% Conf.	Null Hypothesis Rejected
Attempts	$y = 815/(1+e^{(5.96*(x-0.57))})$	0.9079	2.32	2.46 = F <sub>7,22</sub> (.05)	3.76 = F <sub>7,22</sub> (.05)	No
Participants	$y = 10/(1+e^{(23.51*(x-0.55))})$	0.9813	12.36	2.46 = F <sub>7,22</sub> (.05)	3.76 = F <sub>7,22</sub> (.05)	Yes
Successes	$y = 10/(1+e^{(21.72*(x-0.57))})$	0.9864	17.10	2.46 = F <sub>7,22</sub> (.05)	3.76 = F <sub>7,22</sub> (.05)	Yes

**Table 11. Experiment 3, Center Cluster**

#### 4.3.4 Graphical Analysis for Experiment 3 Bottom Cluster

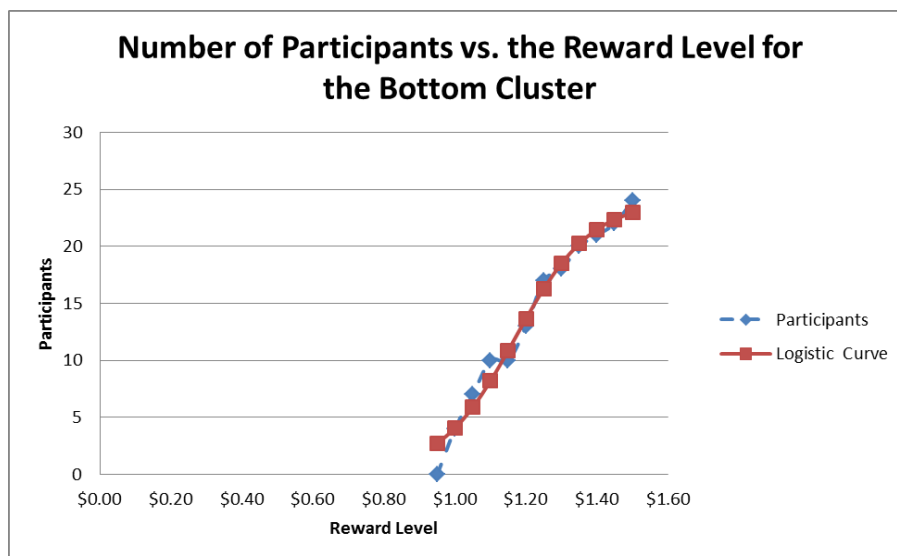
This cluster has 23 participants. Because they did not carry through to the lowest reward level and most quit quite early, the critical value for rejecting the null hypothesis is somewhat higher.

The first graph (Figure 58) shows the number of attempts versus the reward level for this cluster. In this cluster, attempts reject the null hypothesis.



**Figure 58. Experiment 3, Number of Attempts vs. Reward Level for the Bottom Cluster**

Figure 59 shows the number of participants versus the reward level for the bottom cluster. The resemblance to an “S” shaped curve is notable and the results do reject the null hypothesis.



**Figure 59. Experiment 3, Number of Participants vs. Reward Level for the Bottom Cluster**

The number of Successes is graphed in Figure 60. This also shows a significant resemblance to an “S” shaped curve. Statistical analysis on Table 12 shows that these results do reject the null hypothesis.



**Figure 60. Experiment 3, Number of Successes vs. Reward Level for the Bottom Cluster**

Table 12 is arranged in the same manner as Table 2. The critical value for rejection of the null hypothesis is somewhat higher at 2.91.

Experiment Three						
Bottom Cluster						
Measure	Equation	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 98% Conf.	Null Hypothesis Rejected
Attempts	$y = 800/(1+e^{(6.62*(x-1.2))})$	0.8882	3.64	2.91 = F <sub>7,12</sub> (.05)	4.64 = F <sub>7,12</sub> (.01)	Yes
Participants	$y = 24/(1+e^{(9.35*(x-1.17))})$	0.9885	39.55	2.91 = F <sub>7,12</sub> (.05)	4.64 = F <sub>7,12</sub> (.01)	Yes
Successes	$y = 21/(1+e^{(10.36*(x-1.2))})$	0.9880	31.39	2.91 = F <sub>7,12</sub> (.05)	4.64 = F <sub>7,12</sub> (.01)	Yes

**Table 12. Experiment 3, Bottom Cluster**

#### 4.3.5 Graphical Analysis for Experiment 3 Fraternity Cluster

This cluster is unique. During the last day of testing, a student from a business class taught by the proctor of the experiment at the Commons at the University of Idaho, was a participant and scored well, receiving over twenty dollars. He asked if more participants were needed, which they were, and so he called the gentlemen at his fraternity and all that were in the house came over to test. They were well motivated since they decided rather on the spur of the moment to have a party with the proceeds from their testing. They also wanted to look good in front of their fraternity brothers. For this one group, there were good indications that their motivations were high and similar in nature.

There were 13 of them and a couple did go all the way to the end of the experiment. Because of this, their critical value was 2.37 to test the hypothesis.

The first graph (Figure 61) shows the number of attempts versus the reward level for this cluster. In this cluster, attempts reject the null hypothesis.

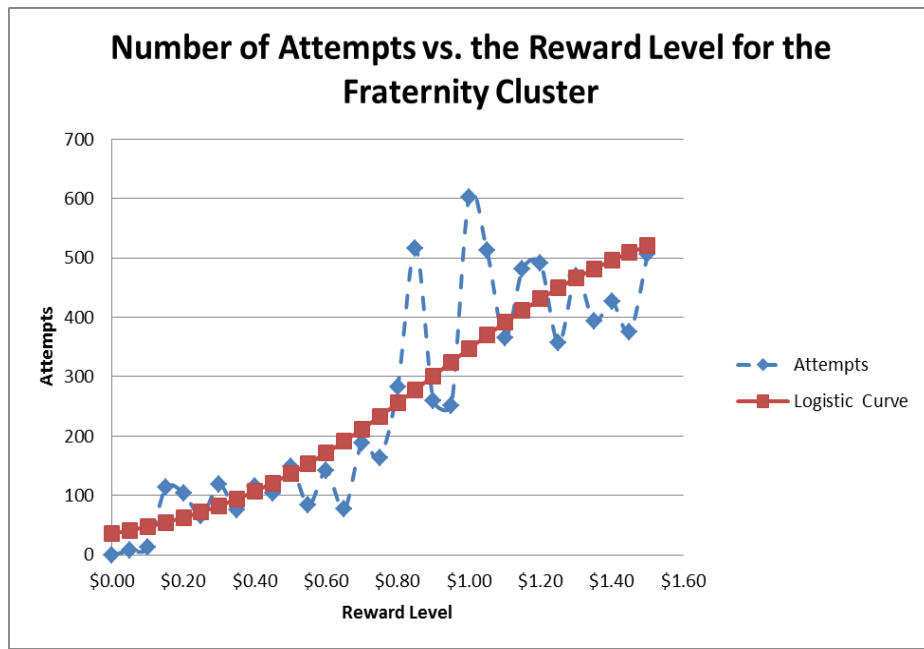


Figure 61. Experiment 3, Number of Attempts vs. Reward Level for the Fraternity Cluster

Figure 62 shows the number of participants versus the reward level for the bottom cluster. The resemblance to an “S” shaped curve is notable and the results do reject the null hypothesis.

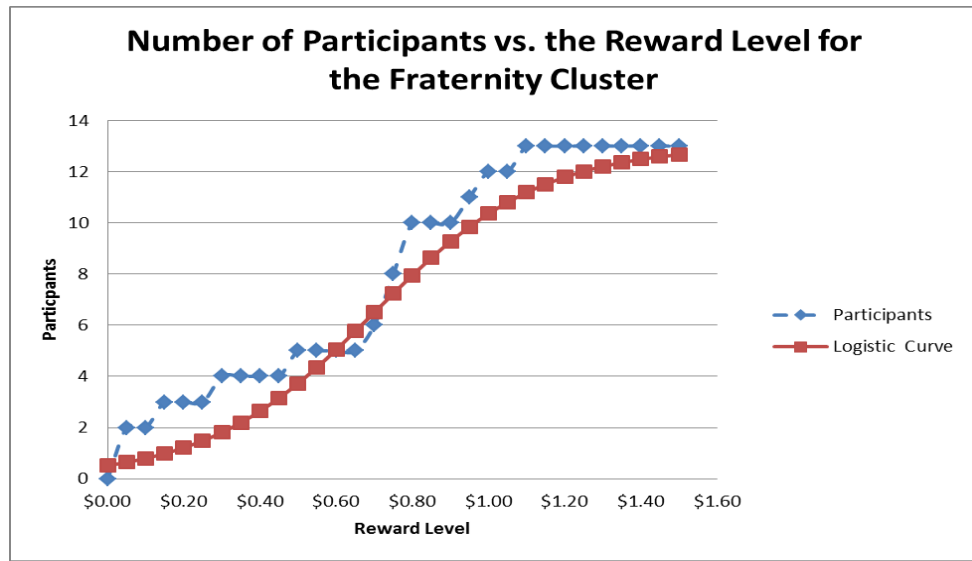
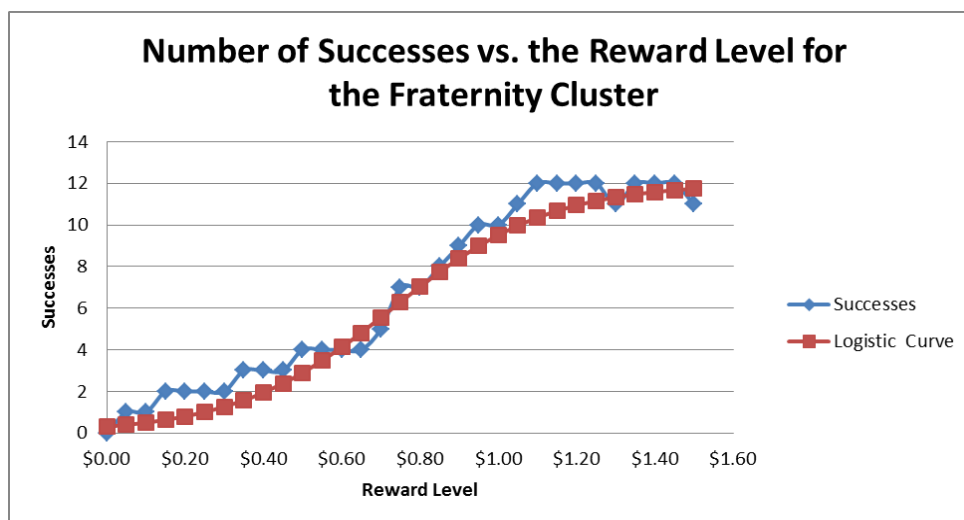


Figure 62. Experiment 3, Number of Participants vs. Reward Level for the Fraternity Cluster

The number of successes is graphed in Figure 63. This also shows a significant resemblance to an “S” shaped curve. Statistical analysis shows that these results do reject the null hypothesis.



**Figure 63. Experiment 3, Number of Successes vs. Reward Level for the Fraternity Cluster**

Table 13 is arranged in the same manner as Table 2. The critical value for rejection of the null hypothesis is somewhat higher at 2.011.

Experiment Three						
Fraternity Cluster						
Measure	Best Fit	R <sup>2</sup>	F value	Critical Value at 95% Conf.	Critical Value at 95% Conf.	Null Hypothesis Rejected
Attempts	$y = 603/(1+e^{(3.07*(x-0.9))})$	0.8772	4.048	2.37 = F <sub>9,21(.05)</sub>	3.40 = F <sub>9,21(.05)</sub>	Yes
Participants	$y = 13/(1+e^{(4.55*(x-0.7))})$	0.9856	36.73	2.37 = F <sub>9,21(.05)</sub>	3.40 = F <sub>9,21(.05)</sub>	Yes
Successes	$y = 12/(1+e^{(4.98*(x-.73))})$	0.9888	47.11	2.37 = F <sub>9,21(.05)</sub>	3.40 = F <sub>9,21(.05)</sub>	Yes

**Table 13. Experiment 3, Fraternity Cluster**

In looking at the Fraternity House cluster it appeared that the number of attempts people were willing to make is statistically higher than in Experiment 1, Experiment 2 or the average for Experiment 3. In Experiment 1, the average number of attempts was 320.5 with



a standard deviation of 239.6. Experiment 2 generated an average of 411.4 with a standard deviation of 247.9. In Experiment 3, the average number of attempts was 500.1 with a standard deviation of 271.22. The Fraternity House cluster had an average of 650.33 with a standard deviation of 178.66. The t obtained when compared against Experiment 1 was 6.658 and when compared against Experiment 2 was 4.684. When it was compared against the average of Experiment 3 the t obtained was 3.033. In this case, the worst critical value is 2.174 (df=22), therefore, the null hypothesis can be rejected, and the average for the fraternity house appears to be statically higher than experiments 1, 2, and 3.

#### 4.3.6 Computer Efficacy

Table 14 below shows the scores for computer efficacy as the previously described cluster within the various experiments.

Experiment	Cluster	Number of Participants	Average Efficacy Score	Standard Deviation	Degrees of Freedom	Student t Score	Critical Value at 95%
1	Top	22	57.5	12.7	21		
1	Bottom	30	53	13.06	29	1.616146318	1.699
2	Top	26	53.8	15.41			
2	Center	10	53.9	12.81	9	-0.014	1.833
2	Bottom	17	53.23	14.99	16	0.266	1.74
3	Top	9	49.75	13.39			
3	Center	17	49.75	15.42	16	0	1.74
3	Bottom	24	46.52	12.96	24	1.220964795	1.711

**Table 14. Efficacy Scores for All Experiments**

None of these student t score reach the critical value for the given degrees of freedom at a 95 percent confidence value inside their experimental boundaries.

## Chapter 5. Discussion and Conclusion

### 5.1 Discussion

One of the most disappointing findings in these experiments was the lack of traction with the measure of computer efficacy. There appears to be no correlation between high computer efficacy scores and the various clusters as shown in Table 14. This measure was thought to have had great potential for such correlation, but apparently one's confidence in computer knowledge does not readily translate to motivation to complete an experiment, even if it is billed as a "Computer Security Experiment." None of the averages of computer efficacy scores between groups is significant. The group that provided the most appreciation of their motives, the fraternity brothers tested in Experiment 3, has an average that is less than a half a point off the mean for that whole population.

Most of the conglomerate graphs and various subgroup graphs displayed characteristics of an "S" shaped curve. The notable exception was the number of attempts in Experiment 2 and to some extent Experiment 3 as shown in Tables 6,7,10, and 11. These graphs had significant variability in the number of attempts at each level. It is possible that some of the participants did not develop a "system" or algorithm to work through the problem in a timely manner and so ran some combinations more than once.

The number of participants and the number of successes, on the other hand, do show consistent "S" shaped curves as described in Tables 2 through 13. It is my opinion that these measures are less affected by the lack of an algorithm on the part of the participants except perhaps those participants who do not develop an algorithm do not last as long.

Unfortunately, data was not collected on the participant's problem solving method so this is only an opinion that needs to be tested. It could also be that the nature of the number of

attempts is just more random and that increasing the sample size by an order of magnitude would also make this measure more consistent. This is also just an opinion.

The demographics of the fraternity house seem to be fairly random, albeit with a higher average attack rate. The demographics of this group show no technical or special mathematic expertise, so they are consistent. It seems apparent that the gentlemen of the fraternity house had a stronger level of motivation and perhaps there was a bit of competitiveness going on. This seems to support the supposition that there are characteristics that can be generalized across a class of attackers. Future experiments will need to have more rigor in determining attacker classes.

These experiments suggest that there is a downward sloping curve as one decreases the reward or increases complexity. Further, most of the curves suggest an “S” shaped curve consistent with other research when the group has some relevant clustering issue that makes them stand apart. Demographics also seem to play a role in the curve and the focus of the attackers.

The support for “S” shaped curves is significant in that these factors can be used to model the behavior of attackers as they try to exploit a given computer resource. These findings seem to support the major assumptions discussed earlier for the original model and so it is more likely that this model can be used to determine some of the characteristics of attackers and selectively harden likely targets or re-educate users to make more efficient use of a scarce security budget.

Modeling of attackers also holds potential for more accurate penetration testing and more realistic security testing in general.

Finally, there is some support for the policy of using a layered security versus a crustal security. The actual hacking task in the second and third experiment required less thought to develop an algorithm to solve it. This is because the number of possible passwords and their configuration did not change. In the first experiment required that they regularly adjust their methodology as one would when attacking a multi-layered defense. When the task did not require constant reevaluation, the participants stayed in longer even though the reward was less as shown in Table 15.

Source	Average	Standard Deviation	Student t obtained
Experiment 1	320.5	239.6	n/a
Experiment 2	411.4	247.9	4.684
Experiment 3	500.1	271.2	3.033
Fraternity House Cluster	650.3	178.7	2.160

**Table 15. Cluster Attempts Comparison**

The third experiment may indicate that a higher reward will motivate attackers to stay in the game longer as the methodology of the experiment was the same, save that the reward was significantly higher (by a factor of more than two) in the third experiment versus the second experiment.

## **5.2 Lessons Learned**

The first lesson learned is that the knowledge about the participants collected in these experiments could have been more in depth. The analysis of these experiments could have been more effective had more been known about the background and motivation of the participants as this data would have helped in clustering the samples.

In the future, a more rigorous questionnaire will be developed. The questionnaire will also be more dynamic; for example, if a salient detail is learned in an initial experiment, changing the questionnaire between experiments will be considered. Because of the concern for biasing the results, the same questionnaire was used on all three experiments, even though by the end of the first experiment, the value appeared to be very limited.

On the other hand, a great deal of anecdotal evidence was gathered from listening to the participants talk as they left. For example, it was possible to determine members of the fraternity house by their greetings and conversations with the proctor and others. It was also possible to gather details about why those who stayed in the experiment longest remained. In the first case the proctor was attuned enough to gather the data in a systematic way; for the other issues, it was anecdotal only. Had it been possible to gather information on why participants left the experiment systematically, it is possible that there would be some correlations there that are not now apparent.

For the next series of experiments, an interviewer or interviewers will be included who will ask each participant a number of pre-scripted questions and have some general discussion with them.

There also needs to be a better method of determining participants' knowledge of computer usage and hacking. This may have bearing on their ability and their willingness to hack but computer-efficacy does not measure this factor effectively. In place of computer efficacy, there needs to be a real hacking knowledge and experience test or measure that can be administered quickly. An experimental framework that was closer to actual hacking tasks might also be more revealing.

### **5.3 Conclusions**

Results suggest that if relevant demographic categories of attackers can be clearly sorted out or other clustering tools used, their responses to changes in security (as described in Experiment 1) and value (as described in Experiment 2 and 3), appear to be an “S” shaped curve.

Another interesting observation is that if participants are required to “rethink” their attack pattern, they are not as persistent. In Experiment 1, when they had to reevaluate their strategy to fit a different password alphabet or password length, their total number of attempts was reduced for similar reward. In Experiment 2, where the problem remained the same and the reward changed, they demonstrated willingness to stay with it longer. The observed data seems to support the observation that layered security or security in depth is better than a tough crustal type of security.

These experiments are using a fairly homogenous population to draw participants from in that they were all young university students. Despite that, we saw groups that demonstrated “S” shaped curves.

Finally, there appeared to be support for the notion that increased motivation on the part of the attacker moves the curve but does not qualitatively change it.

### **5.4 Future Work**

Now that this software environment exists, it will enable several other experiments to be completed as follow-on work including investigations into security usability, a taxonomy of users, and further examination of attacker motivations.

This work is open to several extensions. It would be an interesting experiment to provide participants with a constellation of potential attack sites with known rewards and

difficulties and see which ones they choose to attack and measure their success rate. The level of success could be measured several ways. You could measure total return, total number of successful security tasks, or amount of time engaged.

Another way to examine differing responses to security would be to build a number of Honey Pots with varying degrees of security and measure how many participants attempted each and how much effort they invested. Honey Pots could also be constructed with varying rewards to validate the results of Experiments 2 and 3.

This same framework could be used to explore how users make security decisions by providing work related tasks and then “interfering” with them in the name of security.

An experiment could also be constructed to examine the effects of enforcement by extracting a monetary penalty if a participant were to be discovered while attempting one of these simulated attacks. This methodology, which could help in characterizing system attackers as criminals, is relatively new to computer security but it does open up many new techniques and insights into this area.

Underlying the assumptions about “S” shaped curves tested here are two more basic assumptions, that the measurement of value is a scalar quantity and that users and attackers use the same metric. It is perhaps interesting to speculate about circumstances in which these assumptions are not valid. If, for example, the policy space recognizes a two-variable measure of value such as financial reward and political reward, then these responses would be much more complicated to model. Such a model might permit us to distinguish between different classes of attackers: those motivated by financial reward such as ordinary criminals, and those motivated by political considerations, such as hacktivists or terrorists. It remains to extend those models (and this work) in that fashion.

Similar experiments could be run using an interviewer to find out more details about each participant's motivations, knowledge, and other demographics.

A variation on the experiment above would be to mislead the participants about the difficulty or the reward and measure the same data. The goal here would be to determine if it is perception of difficulty or actual difficulty that forms the basis of attackers' decisions as to which sites are targeted.

A follow-on experiment would be to develop this into a real game and take it to run at DefCon and see if "real hackers" would give the same results as college students.

A further line of study would be to develop a taxonomy of targets and determine if there is a reason or reasons that a certain class of hacker would attack any specific group. This might be facilitated with Honey Pots or a laboratory experiment similar to this one.

It is also possible that with a more rigorous collection of demographic and motivational data, factor analysis could be performed that would shed further light on the different hacker groups and what motivates them.



## Chapter 6. References

- Adam, A., (2004). Hacking into Hacking: Gender and the Hacker Phenomenon. *ACM SIGCAS Computers and Society*, Volume 32, Number 7 (2004).
- Adams, A., Sasse, M., (1999). Users are not the enemy. *Communications of the ACM*, v.42 n.12 pp 40-46, Dec 1999
- Alm, J., (1991). A Perspective on the Experimental Analysis of Taxpayer Reporting. *The Accounting Review*, Vol. 66, No. 3, July 1991, pp. 577-593
- Anderson, R., and Moore, T., (2006). The Economics of Information Security, *Science* 314 (5799) October 27, 2006, pp 610
- Articsoft Limited (2001). *Changing face of web security*, [www.arcticsoft.com/wp-changingface.htm](http://www.arcticsoft.com/wp-changingface.htm), revised May 21, accessed 10 May 2007.
- Becker, G.,(1968). Crime and Punishment: An Economic Approach, *Journal of Political Economy* 78, pp 169-217.
- Bernoulli, D., (1738). Specimen Theoriae Novae de Mensura Sortis. *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, 5, pp 175-192. English translation in 1954 *Econometrica*, 22, 23-36.
- Besnard, D., Arief, B., (2004). Computer security impaired by legitimate users. *Computers & Security*, Volume 23, Issue 3, May 2004, pp 253-264, ISSN 0167-4048
- Bilton, N., (2011). Security Experts Say Police Arrested Wrong Hacker. *The New York Times Bits*, <http://bits.blogs.nytimes.com/2011/07/28/security-experts-say-police-arrested-wrong-hacker/> July 28<sup>th</sup>, 2011. (Downloaded January 10, 2014)
- Bindview. (2005). Retrieved October 15, 2008  
[http://www.bindview.com/Services/RAZOR/Utilities/Unix\\_Linux/ZombieZapper\\_forum.cfm](http://www.bindview.com/Services/RAZOR/Utilities/Unix_Linux/ZombieZapper_forum.cfm)
- Block, M., and Heineke, J.M., (1975). Labor Theoretic Analysis of Criminal Choice. *American Economic Review* 65, pp 314-325.
- Browne, P. S., (1976). Computer security: a survey, *Proceedings of the June 7-10, 1976, national computer conference and exposition*, June 07-10, 1976, New York, New York
- Brunvand, E., (2000). The Heroic Hacker: Legends of the Computer Age. *The Truth Never Stands in the Way of a Good Story*, edited by Jan Harold Brunvand, 170-198 (Urbana: University of Illinois Press). Brunvand, Jan Harold. 2003.

- Cahoy, D., and Min, D., (2004). Using Experimental Economics to Peek into the Black Box of Jury Behavior: A Proposal for Jury Research Reform. *Southern California Interdisciplinary Law Journal*, LJ pp 14: 31.
- Caltagirone, S., Ortman, P., Melton, S., Manz, D., King, K., Oman, P., (2006), Design and Implementation of a Multi-Use Attack-Defend Computer Security Lab. *HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, vol.9, no., pp. 220c- 220c, 04-07
- Carayon, P., (2006). Human factors of complex sociotechnical systems. *Appl Ergon*, pp 37:525–536
- Carbone, M., and Geus, P., (2004). A Mechanism for Automatic Digital Evidence Collection on High-Interaction Honeypots. *Proceedings of the 2004 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY, 10–11 June
- Cardenas, J., Coronado, A., Donald, A., Parra, F., and Mahmood, M. (2012). The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation, *AMCIS 2012 Proceedings. Paper 7. July 29*
- Caldwell, T., (2011). Ethical hackers: putting on the white hat. *Network Security*, Volume 2011, Issue 7, July 2011, pp 10–13
- Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, Volume 14, 2004, pp 65-75
- Cavusoglu, H., Cavusoglu, H., and Raghunathan, S., (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, Vol 47, No. 7, July 2004, pp 87-92
- Christen N., Egelman, .S, Vidas, .T, and Grossklags, J. (2011). It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. *Proceedings of the 15th International Conference of Financial Cryptography and Data Security, March 2011, Gros Islet, St. Lucia.*
- Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MISQuarterly* 13(3), pp 319-340.
- DeLone, W., and McLean, E. (1992). Information System Success: The Quest for the dependent Variable. *ISR* 3(1) pp 60-95.
- DeLone, W., and McLean, E. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *JMIS* 19(4) pp 9-30.

- Department of Justice. (2002). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved January 14<sup>th</sup> 2008. from <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf>.
- Duggan, G., Johnson, H., and Grawemeyer, B. (2012). Rational security: Modeling everyday password use, *International Journal of Human-Computer Studies*, Volume 70, Issue 6, June, pp 415–431.
- Dutta, A., and Roy, R. (2008). Dynamics of organizational information security. *Systems Dynamics Review*, Vol 24, No. 3, (Fall), pp 249-275
- Encyclopaedia Britannica. (2014). Student's t-test. *Encyclopaedia Britannica*. Retrieved from <http://www.britannica.com/EBchecked/topic/569907/Students-t-test> January 15th, 2014.
- Falk C. (2005). Ethics and Hacking: The General and the Specific, Norwich University Journal of Information Assurance, June 2005, Retrieved January 14<sup>th</sup> 2008. from <http://nujia.norwich.edu/index.html/>.
- Farber, D. (2002). Miracle cure for security woes? *ZDNet* August 5th, 2002, Retrieved January 14<sup>th</sup> 2008. from <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2876552,00.html>.
- Farahmand, F. , Navathe, S. , Sharp, G. , Enslow, P. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management*, v.6 n.2-3, pp 203-225, April
- Fraley, C., and Raferty, A. (1998). How Many Clusters? Which Clustering Method? Answers Via Model-Based Cluster Analysis *The Computer Journal* (1998) 41 (8): pp 578-588.
- Freman, E. (2006). Wardriving: Unauthorized Access to Wi-Fi Networks. *Information Systems Security*, Vol. 15 Issue 1, Mar/Apr, pp 11-15
- Forrester, Jay W. (1961). *Industrial Dynamics*, Cambridge MA, MIT Press.
- Garg, A., Curtis, J., and Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security*, March/April.
- Gordon, G.,A., and Loeb, M. P. (2002). The Economics of Information Security Investment. *Transactions on Information and System Security (TISSEC)*. Volume 5 , Issue 4 November pp 438-457.
- Gordon, G., Loeb, M., Lucyshyn, W., and Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey. *Computer Security Institute*.

- Gordon, G., and Loeb, M. (2002). The Economics of Information Security Investment, *Transactions on Information and System Security (TISSEC)*, Volume 5 , Issue 4 November pp 438-457.
- Grossklags, J., (2007). Experimental economics and experimental computer science: a survey, *Proceedings of the 2007 workshop on Experimental computer science*, San Diego CA, Article 11, ISBN 978-1-59593-751-3
- Grow, B., and Bush, J., (2005). Hacker Hunters, *Business Week*, Issue 3935, May 30<sup>th</sup>, pp 74-82
- Hearn, K., Mahncke, R., and Williams, P., (2009) Culture Jamming: From Activism to Hactivism. *10th Australian Information Warfare and Security Conference*, 1st through 3rd December, Perth, Western Australia
- High Performance Systems, IThink / *Stella Technical Documentation*, Lebanon NH.
- Holtzman D. (2003). If You Can't Stand the Heat, Don't Call 'Em. *CSO Magazine*. July.
- The Human Assurances Committee. (2006). Retrieved January 17<sup>th</sup> 2008. from <http://www.webs.uidaho.edu/hac/>
- Jonsson, E., and Olovsson, T. (1997), A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior. *IEEE Trans. Software Eng.*, Apr., pp 235-245.
- Jordan T. and Taylor P. (1998). A sociology of hackers. *Sociological Review* 46#4, pp 757.
- Kagel, J., and Roth, A., (1995). *Handbook of Experimental Economics*. Princeton University Press, 1995
- Karlan, D., (2005). Using Experimental Economics to Measure Social Capital and Predict Financial Decisions. *American Economic Review*, Volume 95, Issue 5, Dec, pp 1688-1699.
- Kelley, M., (2012). There's A Virtual CyberCity Where Government Hackers Train For Real World Attacks. *Business Insider: Military and Defense*, Retrieved Nov 27, 2012 from <http://www.businessinsider.com/cyber-city-built-to-train-government-hackers-2012-11#ixzz2O1gz8T00> Downloaded March 18th, 2013.
- Kenneally, E. (2002). Whos's liable for insecure networks? *IEEE Computer*, pg 93-95, June.
- Kshetri, N. (2006). The Simple Economics of Cybercrimes. *IEEE Security & Privacy Magazine*, Volume 4, Issue 1, Jan.-Feb, pp 33 - 39

- Lee, A., and Bureau, P. (2007). The Evolution of Malware, *as presented at Virus Bulletin Conference*, November, pp 8-10.
- Lakhani, K., and Wolf, R. (2003). Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects. *MIT Sloan Working Paper* No. 4425-03. Available at SSRN: <http://ssrn.com/abstract=443040> or doi:10.2139/ssrn.443040
- Levy, S., (1984). *Hackers*, Anchor Press/Doubleday, New York, New York
- Lewis, J., (2002). *Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats*, Center for Strategic and International Studies, Washington, DC (December 2002).
- Lum, C., and Yang, S. (2005). Why do evaluation researchers in crime and justice choose non-experimental methods? *Journal of Experimental Criminology*, Volume 1, Number 2, July, pp 191-213
- Martinez-Moyano, I., Samsa, M., Burke, J., and Bahadir, A. (2008). Toward a Generic Model of Security in an Organizational Context: Exploring Insider Threats to Information Security, *Proceedings of the 41<sup>st</sup> Hawaii International Conference on System Sciences*, Honolulu, Hawaii
- Mazzetti, M., and Sanger, D. (2013). Security Leader Says U.S. Would Retaliate Against Cyberattacks, *New York Times*, Page A4, March 13<sup>th</sup>
- McDermott J., and Fox, C. (1999) Using abuse case models for security requirements analysis. *Proceedings of the 15th annual computer security applications conference (ACSAC'99)*, Phoenix, Arizona
- metac0m (2003). What is hacktivism? 2.0. retrieved October 5th 2005 from <http://www.thehacktivist.com/hacktivism.php>.
- Mitnick, K., and Simon, W. (2002). *The Art of Intrusion*. Indianapolis In., Wiley Publishing Inc.
- Mosteller, F. and Noguee, P. (1951). An Experimental Measurement of Utility. *Journal of Political Economy*, 59, pp 371-404.
- Mozur, P., (2013). Prime Minister Denies Aiding Cyberattacks. March 18, pp A6, U.S. edition of *The Wall Street Journal*
- Olson, P., (2012). *We Are Anonymous*, Hachette Digital Inc. June 5<sup>th</sup>
- Olavsrud T. (2001). Egghead Files for Bankruptcy, Plans to Sell Assets. Internet News retrieved April 8th, 2013, from [www.internetnews.com/ec-news/article .php/866871](http://www.internetnews.com/ec-news/article.php/866871).

- Pasquali, V., (2013). The Untold Cost of Security. Global Finance, posted May 2013, downloaded from <http://www.gfmag.com/archives/175-may-2013/12482-cover-growing-threat-the-untold-costs-of-cybersecurity.html#axzz2qKOxMfhk> January 13, 2014.
- Pekka, H. (2001). *The Hacker Ethic*. Random House, New York, New York.
- Pendegraft, N., (in press). User Attitudes Toward Password Security: Survey And Simulation, *Journal of Information System Security*
- Pendegraft, N., Rounds, M., and Frincke, D. (2005). A Simulation Model Of IS Security. *43<sup>rd</sup> ACM Southeast Conference*, March 18-20, 2005, Kennesaw, GA
- Pendegraft, N., and Rounds, M., (2006). A Simulation of IS Security with Variable Attacker Populations. *INFORMS Annual Meeting*, November 5-8, 2006, Pittsburg, PA
- 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
- Plott, C., and Smith, V., (2008). *Handbook of experimental economics results*. North-Holland, Amsterdam, The Neatherlands.
- Radcliff, D. (2000). Should You Strike Back? *Computer World*, Nov 13.
- Rajput, S.A., Chen., J., & Hsu, S. (2005). State based authentication, *Proceedings of the 43rd Annual Association for Computing Machinery South East Conference 2*, pp 160-165.
- Reith M, Carr C, Gunsch G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, spring: 1.
- Rhee H., Kim, C., and Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Journal Computer & Security*, vol. 28, pp 816-826.
- Richmond, R (2004). Money Increasingly Is Motive For Computer-Virus Attacks. *Wall Street Journal*, 19 Sept., B5.
- Rosenbaum, P., (2002). *Observational Studies, 2nd ed*. Springer-Verlag, New York, New York.
- Rogers, E. M. (1962). *Diffusion of Innovations*. The Free Press. New York.
- Rosenfeld, S., Rus, I., and Cukier, M., (2007). Archetypal behavior in computer security. *Journal of Systems and Software*, Volume 80, Issue 10, October ,pp 1594-1606

- Rounds, M., Pendergraft, N., and Taylor C., (2007). Human-Centric Approach to Simulation of IS Security Dynamics. *presented at the 18th Annual Information Resources Management Association International Conference May 19-23, Vancouver, British Columbia, Canada*
- Rounds, M., and Pendegraft N., (2009). Diversity in Network Attacker Motivation: A Literature Review. *International Conference on Computational Science and Engineering, Vancouver, British Columbia, Canada* vol. 3, pp 319-323, August 29–31.
- Rousseas, S. and Hart, A. (1951). Experimental Verification of a Composite Indifference Map. *Journal of Political Economy*, 59, pp 288-318.
- Saita, A. (2001). On the Cutting Edge. *Information Security*, retrieved April 8th, 2013, from [http://infosecuritymag.techtarget.com/articles.february01/departments\\_news.shtml](http://infosecuritymag.techtarget.com/articles.february01/departments_news.shtml).
- Saltzer J., and Schroeder, M. (1975). The Protection of Information in Computer Systems. *Proc. IEEE*, vol. 63, no. 9, 1975, pp 1278-1308.
- Sasse, A., (2003). Computer Security: Anatomy of a usability disaster, and a plan for recovery, *Proceedings of CHI 2003 Workshop on HCI and Security Systems*, Fort Lauderdale, Florida.
- Sasse, A., Brostoff, S., and Weirich, D. (2001). Transforming The Weakest Link – A Human Computer Interaction Approach To Usable Effective Security. *BT Technological Journal*, No 19, pp 122-131.
- Satter, R. (2013). Anonymous: Arrests By Interpol Were Result Of Infiltration, *Huffington Post*, February 27th, 2013, Accessed February 27th 2013, from [http://www.huffingtonpost.com/2012/03/01/anonymous-arrests-interpol\\_n\\_1312903.html](http://www.huffingtonpost.com/2012/03/01/anonymous-arrests-interpol_n_1312903.html)
- Schneier, B. (2004). Hacking the Business Climate for Network Security. *Computer*, April 2004, pp 87-89
- Schram, A., (2000). Sorting out the Seeking: The Economics of Individual Motivations. *Public Choice*, [Volume 103, Numbers 3-4 / June, 2000](#), pp 231-258.
- Schwabel, Rohring N., Hall, M., and Scultz, E., (2000). Lessons Learned from Deploying a Honey Pot. *Information Security Bulletin*, CHI Publishing, [chi-publishing.com](http://chi-publishing.com).
- Schwartau W. (2000). Can You Counter-Attack Hackers? *NetworkWorld*. April
- Secure Computing, (2005). *SNAP*. retrieved April 8th, 2013, from <http://www.securecomputing.com/index.cfm?skey=1303>

- Security Systems News (2002).  
www.securitysystemsnews.com/october2002/securitystats/09.ssn.pages.02.pdf,  
accessed 18 Aug 2004.
- Senge, P.M. (1990). *The Fifth Discipline*, Currency Doubleday, New York.
- Senge, P., and Kleiner, A. (1994). *The Fifth Discipline Fieldbook*, Currency-Doubleday,  
New York .
- Shapiro, C., and Varian, H. (1999). *Information Rules*, Harvard Business Press, Boston,  
MA.
- Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security*,  
Volume 2004, Issue 1, January, pp 8-12
- Spitzner, L., (2001). Know your enemy: Honeynets, *Honeynet Project*, April 2001, retrieved  
April 8th, 2013, from <http://old.honeynet.org/papers/honeynet/>.
- Spitzner, L., (2003). *Honeypots: Tracking Hackers*. Addison-Wesley, [Online]. Available:  
<http://www.tracking-hackers.com/book/>
- Stallings, W., (2006). *Cryptography and network security: principles and practice*. Edition:  
4, Prentice Hall, New York, New York.
- Steele, G., and Raymond, E. (1996). *The New Hacker's Dictionary*. 3rd edition, MIT Press.  
Cambridge, MA.
- Stringer, R., (2008). War in the Wires. *Infosecurity*, Volume 5, Issue 6, September 2008, pp  
10.
- Taylor, P., (2005). Hackers to hacktivists: speed bumps on the global superhighway? *New  
Media & Society*. Vol7(5): pp 625-646.
- Taylor, P., (1999). *Hackers: Crime in the Digital Sublime*. Rutledge, London and New  
York.
- Thayer, R. (2005). Hack ... hack back ... repeat. *Network World*. August 9th, 2004,  
retrieved January 19<sup>th</sup>, 2008, from  
<http://www.networkworld.com/news/2004/080904defcon.html>.
- Thomas, T. (2009). *The Bear Went Through the Mountain: Russia Appraises its Five-Day  
War in South Ossetia*, *Journal of Slavic Military Studies*, Taylor & Francis Group,  
LLC, 2009



- Thoras, M., (2013). "The Global Cybersecurity Market 2013-2023",  
MarketinResearchReports.biz, June 13, 2013,  
<http://www.prweb.com/releases/2013/Cybersecurity-Market/prweb10834320.htm>  
Downloaded January 13, 2014.
- Thurstone, L. (1931). The Indifference Function. *Journal of Social Psychology*, 2, 139-167.
- Turgeman-Goldschmidt O. (2005). *Hackers' Accounts: Hacking as a Social Entertainment*.  
Social Science Computer Review, Vol. 23 No. 1 spring 8-23.
- Vympel, M., and Minor, B. (2011). *Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?* Zone-h, June 6<sup>th</sup>, 2011, <http://www.zone-h.org/news/id/4737>. Downloaded January 13, 2014.
- Wait P., (2005). Industry groups urge Senate ratification of cyber crime treaty. *Government Computer News*, June 29th, 2005 retrieved April 8th, 2013, from  
[http://www.gcn.com/vol1\\_no1/daily-updates/36257-1.html](http://www.gcn.com/vol1_no1/daily-updates/36257-1.html)
- Walters D., and Lancaster, G. (1999). Value And Information: Concepts And Issues For Management. *Management Decision*, Volume 37 Issue 8, pp 643.
- Udo, G.J., (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management & Computer Security*, 9, 4, pp 165–174.
- US Department of Commerce (2013). Quarterly Retail E-Commerce Sales 3<sup>rd</sup> Quarter 2013. [https://www.census.gov/retail/mrts/www/data/pdf/ec\\_current.pdf](https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf), Released 22 November 2013, accessed 13 Jan 2014.
- Wallis, A. and Friedman, M., (1942). The Empirical Derivation of Indifference Functions. *Studies in Mathematical Economics and Econometrics*, O. Lange, F. McIntyre, and T.O. Yntema, editors, Chicago, University of Chicago Press, pp 175-189.
- Walters J., Liang Z., Shi W., and Chaudhary V. (2006). Wireless sensor network security: a survey. *Security in distributed, grid, and pervasive computing*. Auerbach Publications, CRC Press,
- Winston, Wayne, (1994). *Operations Research: Applications and Algorithms*, Duxbury, Belmont CA.
- Wixom, B. and Todd, P.(2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. *ISR*,16(1) pp 85-102.
- XLSTAT (2012). Downloaded April 2012, from <http://www.xlstat.com/en/>

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

Young, R., Lixuan, A, and Pributok, V. (2007). Hacking into the Minds of Hackers. *Information Systems Management*, Vol. 24 Issue 4, Fall, pp 281-287

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

**Appendix I**  
Computer Self Efficacy Quiz

**Section 1**

1. What is your Major \_\_\_\_\_?
2. What is your year in school?
  - a. Freshman
  - b. Sophomore
  - c. Junior
  - d. Senior
  - e. Graduate Student
  - f. Other\_\_\_\_\_
3. Gender?
  - a. Male
  - b. Female
4. What is your Age? \_\_\_\_\_
5. Have you ever held a position where one of your major responsibilities was configuring computer systems or networks?
  - a. Yes
  - b. No
6. If the answer to the previous question is yes, what was your job title to the best of your knowledge. \_\_\_\_\_

**Section 2**

Please place a check next to any of the courses below that you have passed?

Math 310 Ordinary Differential Equations  
 Math 385 Theory of Computation  
 Math 386 Theory of Numbers  
 Math 476 Combinatorics  
 Math 578 Combinatorial Optimization  
 Any Senior or Graduate Level Math Class  
 CS 336 Introduction to Information Assurance  
 CS 385 Theory of Computation  
 Any CS Senior Level or Graduate Course  
 Bus 355 Systems Analysis and Design  
 Bus 452 Business Telecommunications Management

**Section 3**

**Rate the following questions using this scale**

- 7 = Strongly Agree  
 6 = Agree  
 5 = Somewhat Agree  
 4 = Neither Agree nor Disagree  
 3 = Somewhat Disagree  
 2 = Disagree  
 1 = Strongly Disagree

- I feel confident handling virus infected files.
- I feel confident getting rid of spyware.
- I feel confident understanding terms/words relating to information security.

- I feel confident learning the method to protect my information and information system.
- I feel confident managing files in my computer.
- I feel confident setting the Web browser to different security levels.
- I feel confident using different programs to protect my information and information system.
- I feel confident learning advanced skills to protect my information and information system.
- I feel confident getting help for problems related to my information security.
- I feel confident using the user's guide when help is needed to protect my information and information system.
- I feel confident updating security patches to the operating system.

**Appendix II**  
IRB Approval

**To:** Mark Rounds  
College of Economics and Business  
University of Idaho  
Moscow, ID 83844-3161

**Cc:** Dr. Norman Pendegraft  
Dr. James Alves-Foss

**From:** Traci Craig, PhD  
Chair, University of Idaho Institutional Review Board  
University Research Office  
Moscow Idaho 83844-3010

IRB No.: IRB00000843

FWA: FWA00005639

Date: June 17, 2010

Project: Approval of "Defining Attacker Behavior Patterns in the Context of an Information System; A Dissertation Proposal" Number 09-239, **Approved June 17, 2010**

---

**On behalf of the Institutional Review Board at the University of Idaho, I am pleased to inform you that the above-named research project is approved as offering no significant risk to human subjects.**

**This approval is valid for one year from the approval date listed above. If you continue with the project after this time, you will need to request extension approval from the IRB committee. Should there be significant changes in the protocol for this project, it will be necessary for you to resubmit the protocol for review by the Committee.**



**Traci Craig**