2005

Modeling End User Behavior to Secure a PC in a Unmanaged Environment

Art Conklin
The University of Texas at San Antonio, art.conklin@utsa.edu

Glenn Dietrich
The University of Texas at San Antonio, glenn.dietrich@utsa.edu

Modeling End User Behavior to Secure a PC in an Unmanaged Environment

Art Conklin
The University of Texas at San Antonio
art.conklin@utsa.edu

Glenn Dietrich
The University of Texas at San Antonio
glenn.dietrich@utsa.edu

ABSTRACT

The concept that central management policies represent the best thinking and model behavior for the operation of the system drives its use in a corporate environment. The majority of home and small business personal computers are operated under conditions that are not governed by a central management policy. Security is still an important aspect to be maintained even if the environment is devoid of central management policies. Responsibility for keeping a system up-to-date falls upon the owner or operator of the system. The desire to maintain an appropriate security posture is based on numerous factors including the user's perception of risk. The development of a model based on the theory of planned behavior, technology acceptance model, and the unified theory of acceptance and use of technology with additional factors for risk is proposed to address this gap in existing theory. This model will lead to a better understanding of user actions with respect to maintaining security on personal computers in an unmanaged setting.

Keywords

Security, technology adoption, technology acceptance

INTRODUCTION

Computer security is rising in importance. Computer security may be centrally managed in corporate and organizational environments, and as such security policies govern individual users. However stand alone PC's are dependent upon end user actions to maintain a proper security posture. The purpose of this research is to examine the factors that influence the adoption behavior of individuals with respect to computer security when they are not governed by central policies. These factors exist in many small enterprises and in home based systems.

According to most popular projections, the global Internet user community will reach over 1 billion users in 2005 with the United States leading the world with over 185 million users. Roughly 70 million of those US Internet users surf the web through high-speed, always-on, broadband connections (Nielsen//NetRatings 2005) – a number that is currently growing by 15% every six months.(FCC 2004) The Internet has become an increasingly hostile environment: identify theft, fraud, corporate espionage, information theft, vandalism, and terrorism are just a few of the traditional threats that have migrated to the digital world.(CSI 2004) Protecting individuals, families, businesses, and the nation from cyber-based threats requires different skills, tools, and capabilities for each group. The list of items from which protection is needed is increasing, with the current threats including viruses, worms, malware, spyware, phishing and now botnet attacks. Some of these attacks are against the user base, and some are against the network or firm. Some of the most dangerous, the botnet attacks, use victim PCs as weapons against other machines and networks. Protection comes in the form of software, but this necessitates users install and maintain the software protection against a constantly evolving threat base.

Keeping machines up-to-date and properly protected against various threats is one of the tasks facing a system administrator. For reasons of efficiency and effectiveness, corporations and organizations typically manage their PC's thus relieving the end user from this responsibility. This is the realm of managed systems, where the specific management tasks associated with system maintenance are delegated to a group that specializes in this functionality. PCs in homes and small businesses do not typically have this type of managed environment and are thus unmanaged with respect to central system administration. For these unmanaged systems, the reliance upon a dedicated system administrator to maintain the system is a less than optimal solution, with issues of training, awareness and importance raising warning flags. With the increasing number of unmanaged PC's being connected to the Internet with high speed, always-on, broadband connections, the scale of threats from these unmanaged resources also grows, threatening all users of the global network.

Security in today's connected environment is a complex issue with technical and behavioral components. Maintaining a system's operating system and application programs through current patch administration is one aspect. Employing anti-virus and anti-spyware applications are another. Maintaining backups of important data files is another as is securing important information with passwords and other security measures. The incorporation of unprotected systems into botnets with the intention of conducting distributed denial of service attacks and other malicious attacks highlights the importance of securing all connected systems.(Clark 2005; Ilett 2004)

The information systems discipline has examined factors associated with how end users embrace new technology at a variety of levels and for a variety of specific system functionality. An example of some of the relevant work includes (Ajzen et al. 1986; Davis 1986; Davis 1989; Heijden 2004; Mathieson 1991; Mathieson et al. 2001; McCloskey 2003; Moon et al. 2001; Venkatesh et al. 2001; Venkatesh et al. 1994; Venkatesh et al. 1996; Venkatesh et al. 2000; Venkatesh et al. 2003; Venkatesh et al. 2002). The vast majority of these studies involve the development of generalizable constructs to explain variance in user behavior with respect to adoption of technology. This study is intended to model user behavior specifically with respect to maintaining a proper security level in their unmanaged systems. Looking at the specific factors that influence end user behavior with respect to what most would consider an insipid task has merit because of the end result of not correctly managing the issue, namely the destruction of the system itself from within.

THEORETICAL FRAMEWORK

This study is posited to apply concepts derived from the various theories associated with user acceptance/adoption of technology in the specific case of applying security functionality in the unmanaged PC environment. The dependent variable is the user behavior associated with applying specific security functionality. The antecedent factors leading to user behavior have been covered in a wide range of studies including TRA/TPB (Ajzen et al. 1986; Fishbein et al. 1975), TAM (Davis 1986; Davis 1989; Gefen et al. 2003; Heijden 2004; Mathieson 1991; Mathieson et al. 2001; McCloskey 2003; Moon et al. 2001; Venkatesh 2000; Venkatesh et al. 1994; Venkatesh et al. 1996; Venkatesh et al. 2002), TAM2 (Venkatesh et al. 2000), UTAUT(Venkatesh et al. 2003). Although the constructs in these previous studies have significance with respect to predicting security functionality, several additional factors are believed to be involved. The role of self efficacy and user experience is also a factor that warrants inclusion. (Compeau et al. 1999; Compeau et al. 1995)

In the definition of the constructs in previous TAM and TAM related studies, the definition of the construct includes an element related to a business use or job aspect. As this research is focused on home use, these constructs have been reworked to more accurately reflect home use issues. The purpose of a PC in the unmanaged environment is also a significant factor to consider in the decision process. A construct to reflect intended usage of the system is included in the models to capture this relevant factor.

The environment under study in this research is that of the unmanaged PC, or more precisely PCs without a central management system. The use of a centralized management system to maintain PCs in a business or organization is for purposes of control and optimization of resources. Centralized management also allows the controlled application of a best practice approach to system management. In the arena of security, this relieves individual users of significant responsibilities and also assists in the application of proper procedures. In the managed environment, specialized resources can be applied to determine and implement a best practice solution with respect to security functionality. This occurs not only at the outset, but can be kept current as operational conditions change over time. In the unmanaged PC environment, this task falls to the end user of the system. The end user may not have all the resources to make a rational decision.

Using the concept of bounded rationality, one can view the user as an agent who faces uncertainty about future events and uncertainty about costs associated with information in the present. (Simon et al. 1958) In a centralized managed environment, an argument can be made for a rational, utility maximizing decision, but in the resource constrained unmanaged environment this is a weak argument at best. There is a large base of empirical literature associated with rational decision making, supporting the implausibility of a highly rational, utility maximizing end user.(Connolly et al. 2002) The unmanaged system user would then make decisions not by optimizing, but by satisficing. As end users are more concerned with the purpose of the PC, their expectations and resource allocation to mundane tasks such as system maintenance may fall short of optimum from a technical best practice standpoint. From the user's view, the solution is still satisfactory as long as the machine functions in the fashion desired. Unfortunately many of the security vulnerabilities and exploits do not immediately expose themselves to the end user until it is too late for correction, if at all. From a modeling aspect, bounded rationality is being incorporated through constructs of experience and self efficacy.

One of the factors that will affect user behavior is perceived risk. The measurement of perceived risk is used in managed systems to determine the appropriate level of resources to apply to a particular aspect of operations. In a managed system, the risk is measured as potential loss to the organization, a multi-dimensional comprehensive measure. For an end user of an unmanaged system, the concept of perceived risk is less comprehensive and typically uni-dimensional related to the loss of functionality of the PC in an immediate sense.

RESEARCH METHODOLOGY

The research methodology being employed in this research is built around model construction and testing using structural equation modeling. Using the previously defined models from the literature review, and extending them to include aspects of perceived risk, knowledge bounds, and experience factors, a series of candidate models is being constructed. For each of the models a set of hypotheses will be developed, explaining the expected relationships between the constructs and the dependent variable. Typical hypotheses include the value of previous computer security experience, either through personal loss or work environment having a positive influence on security adoption. Another is the negative influence that a hedonistic or casual use machine adoption has on the security posture. The constructs associated with these models will be defined in an operational manner that can be measured by survey. A pilot survey will be developed to measure the constructs and tested.

Once a survey is validated, the survey will be applied to obtain data to validate the potential models. The source of data will be a convenience sample of random computer users in the south Texas area. Care will be taken to make this a random public sample and not one biased by occupation or other demographic factors. Demographic data will be collected to validate this assumption. The data will be applied to the models using the method of structural equation modeling. The choice of the best model will be made based on the level of explanation of variance in the system. The results of the fitted model will be used to evaluate the hypotheses.

RESEARCH IMPLICATIONS

The widespread use of PCs, coupled with the Internet has enabled the masses with new functionality. The responsible use of this new medium has many implications. The Internet as currently designed is lacking in systemic security measures. The system as a whole relies upon proper user actions, something that is not being upheld by some groups of malicious users. Although limited in number, these malicious users can unknowingly to the innocent users, corrupt their machines adding to the size of their malicious network. As the Internet depends to a degree on the proper behavior of connected users, the protection of interconnected machines rests upon proper administration of the machine. When this proper maintenance responsibility rests with end users, it is important to understand the factors that shape and influence their behavior. With this understanding, strategies can be researched and developed to assist in securing this vital resource for all users.

REFERENCES

1. Ajzen, I., and Madden, T.J. "Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control," *Journal of Experimental Social Psychology* (22) 1986, pp 453-474.

2. Clark, R. "Remarks at Security Roundtable," RSA Conference, San Francisco, CA, 2005.

3. Compeau, D., Higgins, C.A., and Huff, S. "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quarterly* (23:2), Jun 1999, pp 145-158.

4. Compeau, D.R., and Higgins, C.A. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), June 1995, pp 189-211.

5. Connolly, T., Arkes, H., and Hammond, K. *Judgement and Decision Making:An interdisciplinary reader* Cambridge University Press, New York, 2002.

6. CSI "9th Annual CSI/FBI 2004 Computer Crime and Security Survey," Computer Security Institute.

7. Davis, F. "Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results," Massachussetts Institute of Technology, Boston, MA, 1986.

8. Davis, F.D. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3 (September)) 1989, pp 319-340.

9. FCC "High-Speed Services for Internet Access: Status as of June 30, 2004," Federal Communication Commission, Washington, DC, p. 25.

10. Fishbein, M., and Ajzen, I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research* Addison-Wesley Publishing Company, Reading, MA, 1975.

11. Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in online shopping: An integrated model," *MIS Quarterly* (27:1), Mar 2003, pp 51-90.

12. Heijden, H.v.d. "User Acceptance of Hedonic Information Systems," *MISQ* (28:4), December 2004 2004, pp 695-704.

13. Ilett, D. "30,000 botnets march across the Internet," in: *ZDNet UK*, Barcelona, Spain, 2004, p. 1.

14. Mathieson, K. "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," *Information Systems Research* (2:3 (September)) 1991, pp 173-191.

15. Mathieson, K., Peacock, E., and Chin, W.W. "Extending the technology acceptance model: The influence of perceived user resources," *Database for Advances in Information Systems* (32:3), Summer 2001 2001, pp 86.

16. McCloskey, D. "Evaluating Electronic Commerce Acceptance With The Technology Acceptance Model," *Journal of Computer Information Systems* (44:2), Winter2003-2004, 2003, pp 49-57.

17. Moon, J.W., and Kim, Y.G. "Extending the TAM for a World-Wide-Web context," *Information & Management* (38:4), Feb 2001, pp 217-230.

18. Nielsen//NetRatings "NetView," Nielsen//NetRatings, 2005.

19. Simon, H.A., and March, J.G. *Organization* Wiley, New York, NY, 1958.

20. Venkatesh, V. "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information Systems Research* (11:4), Dec 2000, pp 342-365.

21. Venkatesh, V., and Brown, S.A. "A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges," *MIS Quarterly* (25:1), March 2001 2001, pp 71-102.

22. Venkatesh, V., and Davis, F.D. "Modeling the Determinants of Perceived Ease of Use," International Conference on Information Systems, Vancouver, British Columbia, 1994, pp. 213-227.

23. Venkatesh, V., and Davis, F.D. "A Model of the Antecedents of Perceived Ease of Use: Development and Test," *Decision Sciences* (27:3 (Summer)) 1996, pp 451-481.

24. Venkatesh, V., and Davis, F.D. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," in: *Management Science*, 2000, pp. 186-204.

25. Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), September 2003 2003, pp 425-478.

26. Venkatesh, V., Speier, C., and Morris, M.G. "User acceptance enablers in individual decision making about technology: Toward an integrated model," *Decision Sciences* (33:2), Spr 2002, pp 297-316.