Spring 5-19-2016

Beyond the Prisoner's Dilemma: Using the Game Theory Security Model to Develop Robust Information Security Policies

Alan Rea
Western Michigan University, rea@wmich.edu

Beyond the Prisoner's Dilemma: Using the Game Theory Security Model to Develop Robust Information Security Policies

Alan Rea
Western Michigan University
rea@wmich.edu

ABSTRACT

In this research I explore and apply game theory to security policy creation and maintenance for network, mobile, and Internet of Things systems. After introducing game theory's tenets, I describe the generational development of information security policy and how contemporary socio-technical policy formation fails to address the dynamic nature of ubiquitous computing.

Next I assert that the Game Theory Security Model (GTSM) can protect networked, mobile, and IoT systems from a diversity of cyberattacks. Using the zero-sum game strategy, in which losses are a requirement for wins (Davis, 1983), I propose organizational strategies necessary to achieve a state of pragmatic equilibrium (Gintis, 2009, 2011). Further using this model, I recommend policies an organization can implement to minimize data loss and protect critical systems.

Finally, I will test the GTSM's viability through a series of software implementations in diverse contexts. The paper ends with recommendations for effectively implementing the GTSM.

Keywords (Required)

Security Policy, Game Theory, Ubiquitous Computing

INTRODUCTION

No one questions how ubiquitous computing has transformed business, communication, information, and society. The Internet has birthed innovative cyberjuggernauts such as Amazon, Facebook, and Google, as well as worrisome denizens such as Anonymous, LulzSec, and many others. Ever-expanding interconnectivity is creating a world in which we talk to bluetooth smart watches while commuting in autonomous cars to computer-controlled office environments from our managed networked homes. In such a context I examine how to harness the tremendous opportunities afforded by such technological conveniences while minimizing potential exposure of data, systems, information security and privacy to cyberattack. This is accomplished by using the GTSM.

Security Challenge of IoT

Mobile and Internet of Things (IoT) computing promises even greater B2B and B2C opportunities through powerful targeted advertising. For example, running out of milk will be a thing of the past when grocers can respond to computerized reports of refrigerators' and pantries' deficiencies with automated deliveries. And, no longer be limited to banner-ad-driven cookie information on Web pages, advertisers will customize electronic billboards on the spot given consumers' geolocational data.

But new challenges arrive with the potential use of such an individualized, long tail of advertising and supply chain responses. It requires that businesses first learn how to access and manage exponential amounts of rich information, increased interactivity, and device connectedness. No longer will managers rely on asset tags or RFID; instead, devices will constantly report their own locations. As computers intersect every aspect of consumers' professional and personal lives, successful businesses will respond with contemporaneous, unique advertising and sales possibilities.

Similarly, trust relationships can be hindered significantly when every technology--from pacemaker to power plant--collects and stores data every microsecond. Those who worry about drones flying around in Orwellian fashion will soon also have to cope with public restrooms recommending insurance rate adjustments. Unfortunately, such significant changes to our interconnected world are quickly eroding consumer confidence in the safety of online communications and transactions.

Archaic Defensive Security Policy

Beginning with the digital revolution in the 1970s, and continuing with the proliferation of communication technologies even until present day, security professionals have developed tools and approaches to ensure the confidentiality, integrity, and availability of these systems and the data they contain.

However, the security professional's toolkit has not changed dramatically enough to accommodate contemporary, exponential challenges. This is best illustrated in the cautious evolution of system and security policies (White and Rea, 2003). First-generation system policies consisted primarily of checklists narrowly focusing on "what can be done rather than what needs to be done" (Baskerville 1993, p. 381). Those who counter that these approaches have been abandoned need only to read help desk checklists or user manuals; first-generation policies remain because they are easy for users to follow as long as no outliers cause the steps or checklist to fail. Unfortunately, in the security realm, such inadequate policies are still being advocated in vulnerable areas, such as the relative simplicity of a wireless home router setup.

Second-generation security policies, by contrast, have tried to respond to the complexity of networked business systems. These move from checklists and physical steps to security concepts. Many highly-technical system procedures used today are based on second-generation security policies. Here emerges system requirement specifications such as entity relationship diagrams to determine system and security needs.

This interconnectedness does not automatically imply social connectivity (e.g., shared network printers). To underscore this Baskerville notes that second-generation approaches focus on the mechanistic aspects of systems (Baskerville 1993, p. 400) rather than business process needs that can result in functionality versus security conflicts (Baskerville 1993, p. 401). It is well known that when users are excluded from the system design process that implements a secure mechanism, they often find a "work-around" to speed up tasks or reduce work demands.

Having learned that ignoring human interaction will compromise security, computer professionals developed third-generation policies that considered both behavior and organizational needs (Baskerville 1993, p. 402). One such expansion notes that although Baskerville's model does not fully take into the account what is now considered social, it does address organizational (Siponen, 2001). Therefore Siponen creates a fourth-generational socio-technical approach in which communication among responsible system parties is "understandable for both normal users and system designers – therefore breaking the possible communication gap" (Siponen 2001, p. 115). Siponen better understands the complexity and interconnected system matrices inherent in today's organizational systems.

PROACTIVE GAME THEORY SECURITY MODEL

Yet even fourth-generational approaches rely more heavily on defensive than proactive postures for policy planning. Risk Management security models and other traditional approaches are not effective against ever-changing cyberattack vectors in the interconnected IoT environment.

The solution is the Game Theory Security Model (GTSM). It draws from accepted Game Theory approaches in Economics, Sociology, Biology, and Physics and applies them to the interaction between entities (defender and attacker) starting with the well-known "zero-sum" game that is best illustrated by the classic "prisoner's dilemma" (Von Neumann and Morgenstern, 1964; Luce and Raiffa, 1967). From there the GTSM moves into a mixed strategy and utiles approach to address the dynamic nature of cyber-attacks within varying contexts, most specifically IoT.

GTSM Challenges

Creating an effective GTSM framework offers fascinating challenges. Most significantly, the security attack cannot always be envisioned as a two-sided scenario. In multi-factional attacks, the number of players is unknown as well as the rules by which they play (Camerer, 2003). Security strategies must try to compensate for new malware signatures, social engineering approaches and a myriad of attack vectors. The GTSM model also must deal with this unattainable equilibrium (Siegfried, 2006). How to best accomplish this is a significant portion of the research application component.

GTSM Solutions

Given the challenges facing the GTSM, why bother? Reactionary, defensive strategies that worked in the past are inadequate against today's complex cyberattacks, which have morphed far beyond DDOS or malware. Anti-virus software relying on virus signatures are not useful against zero-day exploits. Previously acceptable protections cannot match multi-pronged attacks against interconnected systems.

Game theory cannot solve all these issues but it can identify players using utiles, minimize losses using equilibrium approaches, handle mixed strategies via minimax, and perhaps attain pragmatic equilibrium. This research determines how to approach these scenarios using a model, and ultimately how to implement that model with effective tools and strategies.

FUTURE RESEARCH DIRECTION

Security and IoT research is a burgeoning discipline with room for those who dissect packets to those who craft policies. The research discussed in this paper has implications for the lowly consumer as well as the multi-national corporation because the digital age is interconnecting everything from cash registers to cars. Protecting valuable data becomes foremost for personal privacy and for international sales. Data breaches destroy not only bank transactions or profits, but just as significantly, they steal the trust necessary for an organization to remain competitive.

To date, GTSM research is placing model discussions within network and mobile security challenges using the zero-sum game approach. Additional research will be necessary to strengthen the model as well as prepare to move into Internet of Things challenges. Now more than ever, proactive models are needed to react to new security challenges in the mobile and IoT sphere. This research is a contribution to that endeavor.

ACKNOWLEDGMENTS

This work was supported by the Haworth College of Business Dean's Summer Faculty Research Fellowship, Western Michigan University.

REFERENCES

1. Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computing Surveys (CSUR)*, v.25 n.4: 375-414.
2. Camerer, C. F. (2003) *Behavioral Game Theory: Experiments in Strategic Interaction*. New York: Russell Sage Foundation.
3. Davis, M. D. (1983) *Game Theory: A Nontechnical Introduction* (Revised). New York: Basic Books, Inc.
4. Gintis, H. (2009) *Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Interaction* (Second). Princeton, New Jersey: Princeton University Press.
5. Gintis, H. (2011) The future of behavioral game theory, *Mind & Society, 10*(2), 97-102.
6. Luce, R. D., and Raiffa, H. (1967) *Games and Decisions: Introduction and Critical Survey* (7th ed.). New York: John Wiley and Sons.
7. Siegfried, T. (2006) *A Beautiful Math: John Nash, Game Theory, and the Modern Quest for a Code of Nature*. Joseph Henry Press.
8. Siponen, M. (n.d.) An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications. In *An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications,* eds. G. Dhillon Hershey, PA: Idea Group.
9. Von Neumann, J., and Morgenstern, O. (1964) *Theory of Games and Economic Behavior* (Science Editions). New York: John Wiley and Sons, Inc.
10. White, D. and Rea, A. (October 2003). The Jing An Telescope Factory (JATF): A Network Security Case Study, *Journal of Information Systems Education*, 14:3, pp. 307-318.