Survivability in Cyberspace using Diverse Replicas: A Game Theoretic Approach

C. A. Kamhoua[1], K. A. Kwiat[1], J. S. Park[2], P. Hurley[1], M. Chatterjee[3]

[1] *Cyber Assurance Branch*
Air Force Research Laboratory, Information Directorate, Rome, New York,
E-mail: charles.kamhoua @ rl.af.mil; kevin.kwiat @ rl.af.mil; patrick.hurley @ rl.af.mil;

[2] *School of Information Studies (iSchool)*
Syracuse University, Syracuse, New York,
E-mail: jspark @ syr.edu;

Abstract: *Survivability represents the quantified ability of a system, subsystem, equipment, process or procedure to function continually during and after a disturbance. Almost invariably, replication of a subsystem or procedure is necessary to meet a system's survivability requirements. Diversity will prevent the same fault or attack from damaging all the replicas so that they can continue the mission. This research shows that the more dangerous vulnerabilities (that affect more replicas) in a system are sometimes less likely to be exploited. This work uses the mathematical framework of game theory to show the significance of replica diversity for mission survival in cyberspace.*

Keywords: *Cybersecurity, Diversity, Game Theory, Replication, Survivability*

Introduction

Today, most system and network operators in an organization (academic institute, industry lab, government facility) deploy fairly homogenous systems primarily because of ease of maintenance, monitoring and upgrades. Homogeneity could provide advantages at the software systems, configuration files, security protection mechanisms, hardware or device level, and network interfaces. However, such homogenous environment also facilitates attackers in concentrating their efforts on just a few types of systems. If the attackers are successful in finding any vulnerability, then they can exploit that to launch an attack that can potentially affect a large number of systems. Thus homogeneity acts as a catalyst that enhances the asymmetric advantages that attackers enjoy today. For example, in May 2012, the Flame virus was declared the most complex malware ever written by researchers at Kaspersky Labs after infecting approximately 1000 machines primarily located in Middle Eastern countries. Flame exploited a flaw in the Microsoft certificate licensing service to propagate and used several novel schemes to avoid detection and gather usage data illicitly. The success of the Flame virus is accelerated by the fact that most computers run identical software to Microsoft.

Approved for Public Release; Distribution Unlimited: 88ABW-2013-2437.

One of the ways to impede attackers is to make the expected payoff much lower than the cost of launching attacks. It is to be noted that attackers would like to use the best possible and most efficient strategies to inflict the maximum damage. Thus, attackers can be discouraged by diversifying the technologies that the systems use. This is because a typical attack exploits a specific vulnerability and different systems are not likely to be affected. For example, if systems were different, the attackers would have to explore additional vulnerabilities as a vulnerability in one system might not be effective in other systems. This diversity would cause impediments for the attackers in two ways: 1.) by increasing their effort required to infect systems, and 2.) by reducing the number of systems that could be infected because of the additional efforts required. In summary, the more diversity is introduced in a system, the less will be the attackerôs payoff from exploiting a systemôs vulnerability. In either case, the return on investment is reduced, making it less profitable to attack.

Generally, although some survivability steps can be applied before an incident, some survivability models are effective after the security mechanisms have failed or after exploitable vulnerabilities have been discovered on a system. By definition, survivability is the capability of a system to fulfill its mission, in a timely manner, even in the presence of attack, failures or accidents. To assure system survivability, replication and diversity become two strong components. Replication will allow the tolerance of the failure to a minimum number of replicas. For instance, a system using five replicas for the same mission will tolerate the failure of two replicas if using a simple majority vote. Diversity will prevent the same fault or attack from damaging all the replicas so that they can continue the mission.
The main contribution of this paper is to provide an analytical modeling of replicas diversity for critical mission survival using game theory. With the increased complexity of cyberspace, cyber survivability will increasingly rely on theoretical models. Analytical and theoretical approaches such as game theoretic modeling provide a general framework that can be applied to numerous problem-specific scenarios. Game theory is the branch of applied mathematics that formalizes strategic interaction among intelligent rational agents. A game theoretic approach is appropriate because the attacks launched in critical systems are becoming more sophisticated and obviously originate from intelligent agents. Moreover, a game theoretic framework can use the Nash equilibrium profile to predict an intelligent attackerôs behavior. This research shows that the more dangerous vulnerabilities (that affect more replicas) in a system are sometimes less likely to be exploited. The attacker may be better off exploiting small vulnerabilities because they will be less protected by the defender. This paper builds upon its preliminary version (Kamhoua, Kwiat, Chatterjee, Park & Hurley 2013) to analyze replica diversity in the framework of game theory.

The remainder of this paper is organized as follows. It will present a background on cyber diversity while emphasizing a few related government research programs. Following that, there will be some related works. After, the authors present their game model and then use a typical scenario to illustrate that game model. Subsequently, the text will also show numerical results that confirm the paramount importance of replicas diversity in a critical mission. Finally, the paper concludes and expresses future research directions.

Background

Homogeneous computational systems provide rich targets for an attacker such that if every machine runs the same software on the same hardware then a single attack exploiting a single vulnerability will compromise all machines. On the contrary, diversity increases system resilience and diminishes the cost of a successful attack. Further, diversity confuses an attacker by making a system more unpredictable. To mitigate the drawback of homogeneous

computational systems (a monoculture), several government agencies have funded over the years research that explore promises of diversity. A few of those research efforts are summarized below.

In 2000, the United States Defense Advanced Research Projects Agency (DARPA) assessed the existing approaches to information system security and survivability ð tenets of high assurance ð as consisting of preventing, detecting and containing unintentional errors and attacks. These systems, by employing static means for high assurance, largely mimicked principles from fault-tolerant computing. The realization that such systems were too vulnerable to attacker-induced faults gave DARPA the impetus to initiate the Organically Assured and Survivable Information System (OASIS) program (Ed. Lala 2003) in partnership with the Air Force Research Laboratoryôs (AFRLôs) Information Directorate. The OASIS program was a cross-disciplinary program that combined fault tolerance and Information Assurance (IA) technologies to build information systems that detect, contain and operate through attacks in the then emerging cyberspace. Following the OASIS programôs successes, a challenge of operating through attacks emerged: resource depletion. Regardless of how well systems are protected or how well they tolerate errors and attacks; they will eventually fail over time unless they have the ability to replenish lost resources. On the positive side, OASIS-type systems that tolerate attacks by gracefully degrading services afford time for these systems to regenerate.

In 2004, DARPA began funding work in Self-Regenerative Systems (SRS) (Online a) aimed at replenishing themselves of losses due to unforeseen errors or attacks and automatically improving their ability to deliver critical services. The SRS program goal was to develop cognitive technologies enabling military systems to learn, regenerate themselves and automatically improve their ability to deliver critical services. Self-regenerative systems show a positive trend in reliability and can actually exceed initial operating capability and approach a theoretical optimal performance level over long time intervals.

The DARPA SRS Program demonstrated Synthetic diversity technology as a useful defense against unanticipated or unimaginable (zero day) technology attacks. Technology attacks exploit programming or design errors; these vulnerabilities are accidently or intentionally (life cycle attacks) introduced by the software builder. Synthetic diversity removes the attacker's assumptions about systems and breaks/disrupts cyber technology attacks. The current state-of-the-art in synthetic diversity techniques (for example, instruction set randomization, address location randomization, stack space randomization, DLL base randomization, heap randomization, encrypted instructions, calling sequence diversity, system call renaming) focus mainly on memory attacks. Existing/practical synthetic diversity techniques provide no coverage for design flaws, algorithm weaknesses, misconfigurations, scripting attacks, data attacks.

In 2006, in order to support the attainment of self-regenerative systems, AFRL embarked upon the óSelf Regenerative, Incorruptible Enterpriseô as a product for Focused Long-Term Challenges (FLTC). The sought-after product would make information systems and data persistent. Such information systems must have redundancy and the ability to regenerate required functionality with increased error and attack immunity, whereby corrupted components can be regenerated without negatively affecting the whole system. The aim of the AFRL effort was to expand replication from being merely large-scale deployments aimed at foiling an attacker with too many targets. By introducing dynamic diversity in runtime

environments, AFRL sought to invoke a machineôs ability to automatically recover from attacks ð demonstrating the passage from fault to attack tolerance.

DARPAôs Clean-Slate Design of Resilient, Adaptive, Secure Hosts (CRASH) program (Online b) seeks to break these intellectual constraints by looking at the problem (as the name implies) from a clean-slate perspective. The goal of the CRASH program is to design highly robust, adaptive and secure computer systems. The CRASH program advocates strategies used by biological systems because they can provide significant inspiration such as in the Human Immune System (HIS). The HIS is composed of multiple redundant mechanisms organized in two layers: innate and adaptive response. The innate response helps avoid, prevent or detect attacks or vulnerability from known pathogens or agents, whereas the adaptive response can learn to recognize new attacks, fight through those attacks and help the body recover or tolerate failure. These mechanisms consume significant resources, but they allow the body to continue functioning and to repair the damage caused by malfunctions and infectious agents.

DARPA launched the Mission-oriented Resilient Clouds (MRC) program (Online c). MRCôs focus is to support mission-oriented computation running on an ensemble of interconnected hosts acting in concert. The goal is to provide resilient support to the mission through adaptation. Loss of individual hosts and tasks within the ensemble is allowable as long as mission effectiveness is preserved. Like CRASH, the aimed-for capabilities of the MRC program include manageable and taskable diversity and moving-target defense. Diversity is recognized as a differentiator from homogeneous computational systems that provide rich targets for an attacker such that if every machine is the same as every other, then a single attack exploiting a single vulnerability will compromise all machines. MRC recognizes that this multiplier-effect for the attacker is magnified in a cloud-computing infrastructure because of the tight integration and the implicit trust typical between hosts within the enclave. A vulnerability shared across a subset of the cloudôs hosts can be exploited and used as a staging base for further attack. The MRC program seeks to develop techniques (and capitalize on techniques from other programs such as CRASH) that make all hosts appear different to the attacker while preserving a common manageability interface. In addition, the program advocates moving target defenses that periodically change the allocation of tasks to hosts, making it difficult for an attacker to ómapô the system well enough to launch a coordinated attack. Since these techniques consume significant resources, the degree to which they are applied is considered a tunable parameter, allowing resources to be used in the most effective manner as the overall threat situation changes. The main objective for this research is to analyze the attack space coverage. This will also improve the ability to protect attack space.

Diversity can also be implemented at various degrees of granularity ranging from coarse-grained system-level diversity to fine-grained (for example, Physically Unclonable Functions (PUF)) component-level diversity. Research on tying mission criticality to the right level of diversity granularity enables a commander to prioritize acceptable levels of diversity and estimate the resulting cost to an adversary to compromise these diverse systems. The approach is to augment the automated code generation process to generate code incorporating the expanded synthetic diversity techniques (for example PUF, model diversity, design diversity, algorithm diversity, data structure diversity, communication protocol diversity, language diversity, operating system diversity, CPU type) to understand their coverage, effectiveness and cost to the adversary. Vogues (1988) presents a survey of software diversity.

Aside from computer system, diversity is an effective strategy in biological systems, agriculture and financial markets. Diversity is achieved in biological systems through random mutation of the DNA molecules. A single pathogen is less likely to contaminate all the individuals in the same species that enjoys genetic diversity and is even less likely to infect two organisms in different species. Diversity aides the resilience of biological systems and with natural selection has been one of the two driving mechanisms of biological evolution. In agriculture, most farmers perceive the risk of a monoculture. A single pathogen can quickly spread a disease in a uniform crop. The entire population of crops can be destroyed in a monoculture because all the plants are genetically similar. However, when a farmer mixes different crops, thus creating a polyculture, it is very likely that one or more variety will be resistant to any particular pathogen. The proverb "Don't put all your eggs in one basket" has always illustrated the importance of diversity in the financial market. For investors, the role of diversity is to protect their investments by minimizing the risk against unpredictable market shocks. Any single stock may drop, but it is unlikely that all the stock in a diversified portfolio would drop at the same time.

Related Works

Interest in using game theory to address network security challenge has increased in recent years. This is because game theoretic modeling favors a comprehensive understanding of strategic cyber interaction. Several types of games have been used depending on the specific scenario. Different scenarios result in distinct game models. Since the attackerôs and defenderôs goals are purely conflicting, zero-sum games are used in Nguyen, Alpcan and Basar (2009) and Kamhoua, Kwiat and Park (2012a). Most game theoretic models assume that all the players are rational. The research presented in Sun, Kong, He, and You (2008) and Kamhoua, Pissinou& Makki (2011) relaxes the assumption of playerôs rationality and uses the mathematical framework of evolutionary game theory to model network security. In some scenarios, the security game is static (Jormakka & Molsa 2005; Liu, Comaniciu & Man 2006); but in others, the game model is repeated, or more generally stochastic (Nguyen, Alpcan & Basar 2009; Shiva, Roy, Bedi, Dasgupta & Wu 2010; Kamhoua, Kwiat and Park 2012b). A stochastic game is a generalization of a repeated game. In a repeated game, players play the same stage game in all periods; whereas in a stochastic game, the stage game can randomly change from one period to the next. Cyber security games also consider what information each player knows. When the rules of the game, and each playerôs strategy and payoffs are assumed to be common knowledge, the cyber game is of complete information as in Jormakka and Molsa (2005). Otherwise, the result is a game of incomplete information that can be formulated as a Bayesian game as in Liu, Comaniciu and Man (2006). The work in Liu, Comaniciu and Man

Liu, Y, Comaniciu, C & Man, H 2006, óA Bayesian game approach for intrusion detection in wireless ad hoc networksô, *ACM International Conference Proceeding Series*; vol. 199.

Myerson R 1997, *Game theory: analysis of conflict*, Harvard University Press, Cambridge, MA.

Nguyen, KC, Alpcan, T & Basar, T 2009, óStochastic games for security in networks with interdependent nodesô, *Proceedings of International Conference on Game Theory for Networks*, GameNets, Istanbul, Turkey, pp.697-703.

Online a, Self-Regenerative Systems (SRS), viewed 28 May 2013, <http://www.tolerantsystems.org/srs.html>

Online b, Clean-Slate Design of Resilient, Adaptive, Secure Hosts (CRASH), viewed 28 May 2013, <http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx.>

Online c, Mission-Oriented Resilient Clouds (MRC), viewed 28 May 2013, <http://www.darpa.mil/Our_Work/I2O/Programs/Mission-oriented_Resilient_Clouds_(MRC).aspx.>

Online d, ó57th Wingô, Nellis Air Force Base, viewed 28 May 28, 2013, <http://www.nellis.af.mil/library/factsheets/factsheet.asp?id=4098>.

Park, J, Kim, S, Kamhoua, C, & Kwiat, K 2012, óOptimal state management of data sharing in online social network (OSN) servicesô in the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-2012), Liverpool, United Kingdom, pp.648-655.

Roy, S, Ellis, C, Shiva, S, Dasgupta, D, Shandilya, V & Qishi, W 2010, óA survey of game theory as applied to network securityô, 43rd Hawaii International Conference on System Sciences (HICSS), Honolulu, HI, pp.1-10..

Shiva, S, Roy, S, Bedi, H, Dasgupta, D & Wu, Q 2010, óA stochastic game model with imperfect information for cyber securityô, 5th International Conference on information Warfare & Security (ICIW), Wright-Patterson Air Force Base, Ohio, pp. 308-318.

Sun, W, Kong, X, He, D & You, X 2008, óInformation security problem research based on game theoryô, International Symposium on Publication Electronic Commerce and Security, Guangzhou City, China, pp.554-557.

Voges, U 1988, óSoftware diversity in computerized control systemsô, *Dependable computing and fault-tolerant systems*, vol. 2, Springer-Verlag Wien, New York.

Author Bios

Charles A. Kamhoua received his B.S. in Electronic from the University of Douala/ENSET, Cameroon in 1999. He received his M.S. in Telecommunication and Networking and his PhD in Electrical Engineering from Florida International University in 2008 and 2011 respectively. He is currently a Research Electronics Engineer in the Cyber Assurance Branch of the U.S.

Air Force Research Laboratory (AFRL) in Rome, New York. His interdisciplinary research area includes game theory, cybersecurity, survivability, fault tolerant networks, and ad hoc networks. Dr. Kamhoua is a member of the National Society of Black Engineer (NSBE). He is the recipient of the National Academies Postdoctoral Fellowship award at the Air Force Research Laboratory, Rome, New York in March 2011.

Kevin A. Kwiat is a Principal Computer Engineer in the Cyber Assurance Branch of the U.S. Air Force Research Laboratory (AFRL) in Rome, New York where he has worked for over 30 years. He received a Ph.D. in Computer Engineering from Syracuse University. Dr. Kwiat holds 4 patents and has published more than hundred journal and conference papers. In addition to his duties with the Air Force, he is an adjunct professor of Computer Science at the State University of New York at Utica/Rome, an adjunct instructor of Computer Engineering at Syracuse University, and a Research Associate Professor with the University at Buffalo.

Joon S. Park is an associate professor at the School of Information Studies (iSchool), Syracuse University, Syracuse, New York, USA. Currently, he is the director of the Certificate of Advanced Study (CAS) in Information Security Management (ISM) at the iSchool. Over the past decades Prof. Joon S. Park has been involved with theoretical/practical research and education in information and systems security. He is Syracuse Universityôs Point of Contact (POC) at the Center of Academic Excellence (CAE) in Information Assurance (IA), which is designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) at the university. He completed his doctorate in the area of information security at George Mason University, Fairfax, Virginia. During his extended sabbatical (Fall 2011 ï Summer 2013), his research has been sponsored by the US National Research Council (NRC), National Academies, as an NRC Fellow.

Patrick Hurley is a Senior Computer Engineer at Air Force Research Laboratory in Rome, New York. He received a Bachelor of Science degree in Computer Science from SUNY Oswego and a Master of Science degree in Computer Information Science from SUNY College of Technology. Mr. Hurley has worked closely with DARPA on various aspects of cyber defence over the past 16 years, especially focusing on survivability architectures, adaptive security, and advanced distributed systems technologies that lead to more agile and better managed systems. Mr. Hurley is currently the lead on two AFRL capability concepts focused on fighting through cyber attacks while maintaining mission essential function. He is a member of the IEEE and has over 20 technical publications.

Mainak Chatterjee received B.Sc. degree (Hons.) in physics from the University of Calcutta, Kolkata, India, in 1994, the M.E. degree in electrical communication engineering from the Indian Institute of Science, Bangalore, India, in 1998, and the Ph.D. degree in computer science and engineering from the University of Texas at Arlington in 2002. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando. His research interests include economic issues in wireless networks, applied game theory, subjective quality-of-service, spectrum management and cognitive radio networks. He serves on the executive and technical program committees of several international conferences.