Winter 12-15-2012

A Structured Approach to Effective Access Control List Tuning

Jordan Shropshire
Georgia Southern University, jshropshire@georgiasouthern.edu

Art Gowan
Georgia Southern University

A Structured Approach to Effective Access Control List Tuning

Jordan Shropshire[1]
College of Engineering and Information Technology, Georgia Southern University, Statesboro, Georgia, United States

Art Gowan
College of Engineering and Information Technology, Georgia Southern University, Statesboro, Georgia, United States

ABSTRACT

Access control lists (ACLs) are rule sets that govern the passing of data packets through network devices such as routers and firewalls. In order to maximize data throughput and minimize security risks, they must be adjusted. The tuning process involves the reconciliation of changed access requirements with the existing rule set, identification of vulnerabilities or performance-degrading rules, and implementation of changes. Informal approaches to this complex task often involve multitasking, a strategy that leads to an increased rate of misconfiguration. To mitigate the impact of perceived task complexity, this research proposes a structured approach to the ACL refinement process. The formalized approach is meant to reduce cognitive overload among information security analysts by sequentially ordering the steps through which an access control list is modified. This work-in-progress also describes an experiment for evaluating the artifact. If supported, it will help IT professionals better secure their infrastructure.

Keywords: Access control lists, refinement process, tuning process

INTRODUCTION

In the information age, the enterprise's information resources are among its most valuable assets. Organizational data must be secured. The first line of defense is the perimeter –

[1] Corresponding author, jshropshire@georgiasouthern.edu +1 912 478 7756

the hardened zone which surrounds and protects the firm's digital assets. This ring must not have any gaps and it must only grant access to authorized users. In this respect, organizations of all sizes face the same problem: differentiating between legitimate and unauthorized traffic. The most common solution is the implementation of an access control list (ACL) (Cavusoglu and Raghunathan 2004). The ACL filters data streams, one packet at a time. It is a logical accompaniment to software and hardware firewalls, routers, servers, and other gateway devices which control network access (Adiseshu et al. 2000). An ACL is applied to a device interface. Separate lists are used to sort incoming and outgoing traffic. Thus, a single firewall may incorporate several access control lists. ACLs are "living" files in that they must be frequently retooled to reflect changes in infrastructure, software, users, and traffic patterns. Out of date ACLs pose tremendous security risks.

ACL refinement is an abstract task. It requires identification and synthesis of access requirements, integration of derived requirements with existing rules, detection of inherent vulnerabilities, and detection of performance inhibitors (Jin-Hua et al. 2008). Informal approaches to ACL revision often involves multitasking – simultaneously considering several sources of data while evaluating the utility of access rules (Ishizaka et al. 2001). Based on previous studies, this manuscript argues that such approaches are error-prone, and likely to create vulnerabilities (Just and Carpenter 1992). Multitasking approaches require the ability to simultaneously consider many pieces of information at a time. They lead to great error rates because it is easy to lose track of details and overlook potential threats. Thus, this research proposes a structured process for ACL tuning which incorporates sequential analysis instead of multitasking. It consists of five steps: information gathering, rule development, comparison, reconciliation, and rule ordering. Its purpose is to derive a more effective ACL while maximizing

analyst efficiency. Following the background section, this manuscript describes the proposed approach. In the methods section, a test of the artifact's effectiveness is described.

BACKGROUND

Access control systems have a history grounded in mathematically-oriented approaches to modeling security policies. Their development and implementation is "multi-phased" and complex (Samarati and Vimercati 2001). But there is relatively little research on the process of ACL development. Research within the information system field has focused on configuration management (Ogut 2012). For instance, one study analyzed the negative consequences of misconfiguration of security devices such as firewalls and intrusion detection systems (Cavusoglu et al. 2009). Another applied decision theory to configuration of IDS software (Cavusoglu and Raghunathan 2004). However, it did not focus on ACL development. Other studies have been conducted within the computer science research tradition. This stream focuses on automating the process of rule construction (Yue and Bagchi 2003). It has led to the development of software which can observe traffic patterns, identify networked services, employ decision rules to identify legitimate traffic, and infer rule sets (Golnabi et al. 2006).

In general, the findings indicate that software is very good at optimization (Samarati and Vimercati 2001), but less effective at locating holes in the perimeter (Ogut 2012). In some cases, automated approaches were found to generate more problems than they solved (El-Atawy 2007). For instance, the algorithms in software-based approaches can be manipulated by sophisticated hackers to create weakened rule sets (Jin-Hua et al. 2008). Aside from technical limitations, algorithmic approaches to ACL tuning present a number of other concerns. Software carries implementation costs. Time, money, infrastructure, operator training, and ongoing support would need to be dedicated to a new program (which is used to configure another program). This

defeats the purpose of static access control lists, which should be straightforward to implement and less reliant on other systems. Even if a software approach is implemented, a member of the IT security team would still need to validate the derived list (Adiseshu et al. 2000). Thus, in many cases, an analyst-derived rule set is preferable.

CONCEPTUAL DEVELOPMENT

The research proposes a structured process for refining access control lists (ACLs). Its purpose is to reduce task complexities perceived by those who tune ACLs, so that they are free to perform deeper, more thorough evaluations. If successful, this artifact will provide significant value because it does not rely on strategies of data recall and triangulation. When multiple sources of data are simultaneously considered, the probability of overlooking critical details increases (Just and Carpenter 1992). This effect increases as the working memory is over-allocated and the recall ability diminishes (Barrett et al. 2004).

The proposed approach is broken into five steps: information gathering, rule development, comparison, reconciliation, and rule ordering. Instead of a multi-tasking approach, the proposed steps are to be executed sequentially with minimal backtracking (Ishizaka et al. 2001). The approach is service-oriented and deny-oriented in that it focuses on controlling access to networked services and is biased to access denial. It is similar to the waterfall model of systems development in that it forces exhaustion of one step before proceeding to the next. This inhibits multitasking and frees the analyst to focus deeper on the problem space (Spink 2004). Table 1 (below) shows more detail regarding the steps.

Table 1. Structured Approach to ACL Tuning

Step	Process	Overview
1.	Information Gathering	Identify the exterior access requirements for networked information services. Determine the characteristics of the packets which should be allowed to pass. Include information such as protocol, source and destination IP address, port number, and flags.
2.	Rule Development	Translate access requirements into access rules according to the syntax requirements of the given platform.
3.	Comparison	Compare the derived rule set against the existing rule set. Use the following three steps to identify rules which should be added as well as those which should be stricken. First, determine which of the newly-created rules are contained in the existing rule set. Second, if a rule is not represented, determine if the access requirement is met through a combination of rules in the old ACL. Those not represented should be added. Third, analyze remaining rules in the old rule set to determine purpose.
4.	Reconciliation	Combine the two lists into a single ACL. Focus altering the in-place ACL rather than implementing an entirely new ACL. Incorporate newly-developed rules not previously represented. Strike rules which are no longer applicable
5.	Ordering	Reorganize the list for maximum efficiency. Minimize delay by dropping as many packets as possible early in the process.

METHODOLOGY

The purpose of this research is to improve the process through which analysts reconfigure access control lists. The previous section proposed a structured analytical approach to arrive at a more secure, efficient ACL. This portion of the manuscript describes an experiment to test the

aforementioned artifact. It uses a randomized Solomon four-group design to identify differences in performance. For this study, the subjects are undergraduate IT majors with between 90 and 120 credit hours and a concentration in network and data center management. As a means of further specification, they must have completed at least once course in network design or architecture. The composition of this sample sacrifices a small degree of realism for rigor. Although the subjects do not have significant work experience they form a relative homogenous group. In turn, this adds credence to the results of empirical tests. Power analysis indicates that a confidence level of .05 can be achieved through n=74. Thus, the estimated sample size will be between 75 – 90 subjects.

The four group design (shown below) includes two experimental groups and two control groups. The groups are of relatively equal size. All four groups complete the post test. Only groups E_1 and C_1 receive pretests. This allows for controlling the effects of pretests. The experimental groups are exposed to the structured ACL tuning process in a thirty minute training session. Fifteen minutes are dedicated to presenting the structured method and fifteen minutes are given to covering an example.

Group	**E_1**	**E_2**	**C_1**	**C_2**
Pretest	X		X	
Treatment	X	X		
Posttest	X	X	X	X

Figure 1. Solomon Four Group Research Design

The pretests and posttests both follow the same procedure. Each subject completes a tuning test in one of five isolated breakout rooms. Each room is equipped a table, chair, whiteboard, and a computer with Internet access. Subjects are given permission to access the Internet to assist in their tuning but are asked not to contact others during the test. This is

checked by monitoring Internet usage; cellular phones were not allowed in the breakout rooms. Each breakout room contains several rack-mounted servers offering various utilities. This equipment requires no configuration. Full connectivity is arranged using two switches and a router. Finally each room contains a Cisco 5500 Series Enterprise Grade Adaptive Service Appliance (ASA) with a preconfigured firewall. The firewall is implemented on the external interface and set to monitor incoming traffic. It has ADSM (Adaptive Security Device Manager) enabled to allow subjects to manage the access control list via a Web GUI.

After completing the ACL revision, subjects are asked to complete a pen and paper survey to provide demographic information and indicate the degree of complexity they perceived in the task. Perceived task complexity is operationalized using a 20-item scale adapted from Nadkarni and Gupta (2007). In the posttest subjects in the experimental pool are also asked to indicate if they used the structured approach to ACL tuning. This information is used as a control. Those who do not perceive complexity will not be included in the analysis. Further, subjects from treatment groups who did not use the artifact (but received training) will be excluded. The dependent variable is measured in terms of analyst performance at ACL tuning. This is assessed via a composite of three measures: time to complete the tuning process, technical errors remaining in the ACL, and data throughput. The mean gain scores for subjects in groups E_1 and C_1 are used in ANOVA calculations. The results compare the effectiveness of subjects using the structured approach against those using informal methods.

CONCLUSION

This work-in-progress focuses on developing an improved method by which analysts can tune access control lists. It presents an artifact that is meant to alleviate the complexities associated with complicated revision scenarios. The structured approach incorporates five

distinct steps, each of which is completed sequentially in order to minimize multitasking and free working memory for more advanced analysis. It proposes an experiment to test the artifact in a controlled laboratory environment. The Solomon Four Group design is employed, and pretests and posttests are designed to reflect an accurate simulation of a system data center. In the future, we intend to test and refine the process so that it may be disseminated among practitioners in order to improve this portion of the perimeter hardening process.

REFERENCES

Adiseshu, H., Suri, S., and Parulkar, G. 2000. "Detecting and Resolving Packet Filter Conflicts," *INFOCOM*, pp. 1203-1212.

Barrett, L., Tugade, M., and Engle, R. 2004. "Individual Differences in Working Memory Capacity and Dual-Process Theories of the Mind," *Psychological Bulletin* (130:4), pp. 553-573.

Cavusoglu, H., and Raghunathan, S. 2004. "Configuration of Detection Software: A Comparison of Decision and Game Theory," *INFORMS Decision Analysis* (1:3), pp. 131-148.

Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. 2009. "Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," *Information Systems Research* (20:2), pp. 198-207.

El-Atawy, A. 2007. "An Automated Framework for Validating Firewall Policy Enforcement " *POLICY '07 Eighth International Workshop on Policies for Distributed Systems and Networks*, Bolonga, pp. 151-160.

Golnabi, K., Min, R., Khan, L., and Al-Shaer, E. 2006. "Analysis of Firewall Policy Rules Using Data Mining Techniques," *10th IEEE Network Operations & Management Symposium*, Vancouver, BC, pp. 305-315.

Ishizaka, K., Marshell, S., and Conte, J. 2001. "Individual Differences in Attentional Strategies in Multitasking Situations," *Human Performance* (14:4), pp. 339-358.

Jin-Hua, W., Xiao-Su, C., Yi-Zhu, Z., and Jun, N. 2008. "A Flexible Policy-Based Firewall Management Framework " *International Conference on Cyberworlds*, pp. 192-194.

Just, M., and Carpenter, P. 1992. "A Capacity Theory of Comprehensionl Individual Differences in Working Memory," *Psychological Review* (99:1), pp. 122-149.

Ogut, H. 2012. "The Configuration and Detection Strategies for Information Security Systems " *Computers & Mathematics with Applications* (In Press).

Samarati, P., and Vimercati, S. 2001. "Access Control: Policies, Models, and Mechanisms," in: *Foundations in Security Analysis and Design,* R. Focardi and R. Gorrieri (eds.). New York, NY: Springer-Verlag.

Spink, A. 2004. "Multitasking Information Behavior and Information Task Switching: An Exploratory Study," *Journal of Documentation* (60:4), pp. 336-351.

Yue, W., and Bagchi, A. 2003. "Tuning the Quality Parameters of a Firewall to Maximize Net Benefit," *Distributed Computing - IWDC 2003*, Berlin, pp. 321-329.