*i*Conference 2009
iSociety: Research, Education, Engagement

Roundtable Discussion

Feasibility Discussion on Identifying Possibility for a National Behavioral Anomaly Detection Platform

Proposed by: Shuyuan Mary Ho† [1]
smho@syr.edu
School of Information Studies
Syracuse University

Joseph Vincent Treglia
jvtregli@syr.edu
School of Information Studies
Syracuse University

Abstract

The purpose of this panel is to identify and discuss high-level parameters and social issues regarding the implementation of a national behavioral anomaly detection platform. This platform would provide a "statistical firewall" to protect the rights of individual privacy, while also supporting the government's obligation to protect the populace. We plan to initiate discussion of investigating the development of a framework to identify potentially incidences of malicious behavior, patterns or activity across a wide variety of industries through an automated analysis of data anomalies from multiple data sources. The result of this panel discussion would be an evaluation of feasibility, of standardized inputs, further definition on the framework and engine, and the identification of the legal and social issues attending such a capability.

[1] † Corresponding author.

1 Introduction

In the world of corporate information security, many countermeasures have been designed and developed to guard against threats from outsider attacks. But it is become obvious that threats from insiders can have a far greater negative impact, and are even more subtle and complex. In corporate environs, personnel that are considered trusted corporate assets generally have valuable corporate knowledge that – if used improperly - could significantly impact profits, or put intellectual property at risk. According to the 2007 CSI Survey, financial losses caused by computer crime have soared to $67 million in 2007, up from $52.5 million in 2006 (Richardson, 2007, pp. 14-15). Nearly 37 percent of respondents attributed more than 20 percent of losses to be caused by insiders. This indicates an increase of insider abuse within network resources from 42 to 59 percent (pp. 12-13) compared with 2006 CSI/FBI Survey. While an employees knowledgebase is essential to the productive operation of an organization, their inside knowledge of corporate resources can also threaten corporate security. Such improper uses are often termed by security experts as the "insider threats" (Moore, Cappelli & Trzeciak, 2008).

In the larger society, there is a similar and analogous need to protect the general populace against criminal and terrorist activities. But the privacy needs of the individual must be balanced against the government's responsibility to protect its people. Identifying and detecting anomalous behavior indicative of criminal or terrorist actions can provide significant protection against potential threats in both corporate and governmental situations, while maintaining the sovereignty of individual activities.

In this discussion, insider threats are identified as one of the significant problems to corporate security, but the same pre-diagnostic solution can also be applied to identify and possibly prevent criminal activity and societal terrorism. Being able to provide early warning signs of possible human threats can be valuable, even if only on a cursory level. Once meta-patterns of behavioral profiles are established, actual data points that represent related human activity can be compared through programmed algorithms - and anomalous behaviors can be identified and flagged for further analysis and consideration. By looking at observable aggregated behaviors the individuals are shielded from scrutiny during the investigative process without sacrificing the security needs of the larger population.

We plan to discuss the possibility of identifying parameters for building a comprehensive behavioral anomaly detection platform that will auto-analyze large amounts of data in such a way as to protect the populace from undue oversight while still providing a way of identifying potential threats. The platform will seek to identify patterns of data anomalies that fall within certain tolerances – and "flag" those patterns that include outliers to such an extent that they require advanced analysis and perhaps human intervention. The national behavioral anomaly detection platform will serve as a statistical firewall, maintaining individual privacies while also enhancing the ultimate security of the larger population. This platform will have potential for countering insider threats within the government, as well as terrorist activities.

2 Research Challenges

The problem of identifying human threats requires inputs and analyses from many systematic and social perspectives. The goal of such analyses is to identify anomalies when compared to normalized behavior patterns. However, simply profiling or monitoring an individual's behavior for the sake of guarding against maliciousness is not an optimal solution. The act of monitoring and surveillance tramples the individual privacy, and can result in distrust or suspicion from the institution toward its constituents (Kramer, 1999, p. 587-589; Cialdini, 1996) Organizational distrust behaviors toward its employee may cause low morale and reduced work ethics in a workplace. The act of institutional distrust may result in a negative cycle that de-motivates employees' engagement and commitment to the organization, because they know that they are monitored (Stanton & Stam, 2006).

The need to understand early warnings of possible human threats is critical. On the other hand, the need for individuals to be free from constant monitoring, and the need to protect human's right to privacy is also inherently important. This then leads to the need for a platform that can calibrate human activity profiles, and is able to provide some level of accuracy in detecting and analyzing anomalous activities. A high level of automation and encryption is required to ensure both individual privacy and organizational security. This platform would also require activity (data) inputs from many other "modules" from a wide spectrum of agencies.

Several research projects have focused on the problem of corporate insider threats. For example, multi-disciplined research using natural language processing techniques, social network analyses and composite role-based monitoring has been studied (Park & Ho, 2004; DelZoppo, et al., 2004). From a social psychological perspective, an individual's trustworthiness can be attributed by "human sensors" in a close relationship (Ho, 2008a). This type of attribution of trustworthiness can be converted to a potential computational module that can be plugged in to the behavioral anomaly detection platform. Likewise, there will be plug-in modules from credit organizations, travel agencies, credit card companies, banking, etc. in order to reflect someone's financial stability. Moreover, there will be encrypted inputs from phone companies, telecommunication service providers and law enforcements as well. These modules can be standardized; plug-in interfaces, inputs and parameters can be specified and encrypted. We must look at alternative governance or participation structures to find one most suitable for purposes here (Brafman, 2008).

3 Initial Idea for the Framework

The purpose of this panel is to discuss and identify inputs to a platform that would predict potential threats by analyzing data-based anomalies which reflect unexpected behaviors as early warning signs.

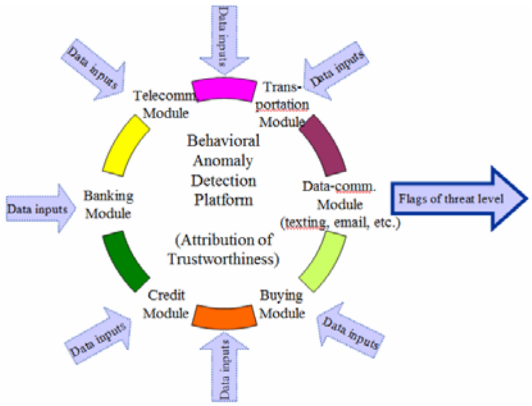

Figure 1: An illustration of a very basic behavioral anomaly detection platform

Categorization of Behavioral Meta-Pattern:

Threat $_{\text{information type, module-1}}$ = { (BP_1, impact), (BP_2, impact), (BP_3, impact), etc. }
Threat $_{\text{information type, module-2}}$ = { (BP_1, impact), (BP_2, impact), (BP_3, impact), etc. }
BP = behavioral pattern

Table 1: An illustration of categorization of behavioral meta-pattern

Figure 1 illustrates the need for standardized inputs and interface for different modules from stakeholder organizations, such as credit union, banks, phone companies, airline companies, email/data/text service providers, etc. Table 1 illustrates the preliminary categorization of behavioral meta-pattern.

4 Panel Discussions Question

We propose to discuss technical, social and policy issues surrounding the implementation of a national behavioral anomaly detection platform and to define its scope and parameters more clearly and universally. Specifically;

1. What parameters can be identified for the use in a behavioral anomaly detection platform for identifying the potential for criminal and terrorist activity?
2. What partnerships with public and private agencies or organizations must included as providers of information for this purpose to be effective?
3. What would the optimal governance structure be for such a platform, and who would control / manage it?
4. What are the legal and policy considerations that must be taken in to account, or changed to make such a system possible. Can it be done under current law and conditions?
5. What are the social implications or requirements for acceptance by the public of such a system platform?
6. What technical safeguards would be required?
7. How would participants in the system be identified and screened for participation or access to the system or its data - as either contributors or end-users?
8. How timely must the data be to be of value to a platform, and how will it be collected and updated?

9. How much interoperability will be required for such a platform to be effective, and how will the technical specifications for interoperability be determined?
10. What will be the process that follows identification of a suspicious or flagged incidence pattern, and who must be involved?

5 Method

A roundtable discussion will be utilized to navigate the issues. Attendees will be invited to discuss possible parameters that will be important to track individual activities without actually tracking individuals. The result of this panel discussion attempts to initiate the discussion on identifying some high-level parameters of the data inputs.

6 Conclusions and Contributions

This study is to consider the feasibility and issues surrounding a nation-wide behavioral anomaly detection platform that collects and analyzes data from among a wide variety of disparate industries, public and private sources. This attempt is at the initial stage of building a framework that will generate early warning “flags” of identified behavioral anomalies at the national level. The potential of this study will contribute to building a statistical and information based firewall that protects human privacy as well as the national security.

Acknowledgements We thank Jeffrey M. Stanton for his constant support and insight. We also thank Conrad Metcalfe for his helpful comments and editing assistance.

6 References

Cialdini, R. (1996). The Triple Tumor Structure of Organizational Behavior, in D. M. Messick and A. E. Tenbrunsel (eds.), *Codes of Conduct*, New York: Russell Sage.

DelZoppo, R., Browns, E., Downey, M., Liddy, E. D., Symonenko, S., Park, J. S., Ho, S. M., D’Eredita, M. and Natarajan, A. (2004) “A Multi-Disciplinary Approach for Countering Insider Threats.” Workshop on Secure Knowledge Management (SKM), Amherst, NY, September 23-24, 2004.

Brafman, O. B. R. A. (2008). *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (p. 240). Portfolio.

Ho, S. M. (2008a). Attribution-based Anomaly-Detection: Trustworthiness in an Online Community. *Social Computing, Behavioral Modeling, and Prediction*. Springer: January 2008, 129-140.

Ho, S. M. (2008b). *Towards a Deeper Understanding of Personnel Anomaly Detection*. Encyclopedia of Cyber Warfare and Cyber Terrorism, 2008 IGI Global Publications, Hershey, PA.

Kramer, R. M. (1999). Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions, *Annual Review of Psychology*, 50(1), February 1999, 569-598.

Lazarevic, A., Ozgur, A., Ertöz, L., Srivastava, J., & Kumar, V. (2003). “A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection,” *Proceedings of the Third SIAM Int'l Conf. Data Mining,* 2003.

Moore, A.P., Cappelli, D.M., and Trzeciak, R.F. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructure. CERT Tech. Report, CMU/SEI-2008-TR-009, May 2008.

Park, J. S., & Ho, S. M. (2004). Composite Role-based Monitoring (CRBM) for Countering Insider Threats. *Proceedings of Second Symposium on Intelligence and Security Informatics* (ISI), Tucson, Arizona, June 2004.

Richardson, R. (2007). 2007 *CSI Computer Crime and Security Survey*. Computer Security Institute.

Stanton, J. M., & Stam, K. R. (2006). *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust*. Medford, NJ: Information Today, Inc.