MIS Quarterly

RESEARCH ARTICLE

INSIDER THREATS IN A FINANCIAL INSTITUTION: ANALYSIS OF ATTACK-PRONENESS OF INFORMATION SYSTEMS APPLICATIONS

Jingguo Wang
Information Systems and Operations Management, College of Business, University of Texas at Arlington,
Arlington, TX 76019 U.S.A. {jwang@uta.edu}

Manish Gupta and H. Raghav Rao
Management Science and Systems, School of Management, State University of New York at Buffalo,
Buffalo, NY 14260-4000 U.S.A. {mgupta3@buffalo.edu} {mgmtrao@buffalo.edu}

Appendix A

System Architecture and Functionality of SiteMinder Web Access Manager (WAM)

WAM is an enterprise single sign-on (ESSO) system providing centralized authentication, authorization and auditing to those integrated web-based applications and portals. It consists of three core components:

1. Policy Server: This component provides centralized policy management and decisions on authentication and authorization requests made by WAM agent on behalf of the users attempting to access protected resources. The policy server performs key security operations including the following:
   - Authentication—The policy server supports a range of authentication methods. It can authenticate users based on user names and passwords, via tokens, using forms-based authentication, or through public-key certificates.
   - Authorization—The policy server is responsible for managing and enforcing access control rules established by the policy server administrator. These rules define the operations allowed for a user on each protected resource.
   - Administration—The policy server allows for creation and management of authentication and authorization rules for protected web applications. This information is used whenever a user attempts to access a protected application.
   - Accounting—The policy server generates log files that contain auditing information about the events that occur within the system. These logs can be printed in the form of predefined reports, so that security events or anomalies can be analyzed.

2. Agent: Installed and configured within the context of a standard web server or application server, agents enable SiteMinder to manage access to Web applications according to predefined security policies.

3. Policy Store: This is a repository where all the information managed by the policy server resides.

Figure A1 illustrates an example of the interaction between different components of the system. A user accesses a web resource (typically a web application) through an Internet browser. All requests for application resources will be intercepted by the Siteminder agent installed on the web server running the application before going to the application. The agent will query the policy server to check whether the requested resource is protected or not. If the resource is protected, it will show the user a login page for him/her to enter credentials such as a user name and password. The agent then passes this information to the policy server, which checks a configured user directory for correctness of the user name and password. At the same time, the policy server also looks up the policy store to retrieve any authorization information. If the user is authenticated (i.e., the supplied credentials are correct), the agent passes the authorization information to the application to restrict the privileges of the user. The session is created (commonly through a transient browser-resident cookie) for the user. For any subsequent access to different resources of the application, the agent queries the policy server for an authorization decision. A cookie is also used to create a single-sign-on experience for the user. For example, if the user tries to access protected resources in a different application, the agent running on that server validates the cookie in the browser. If the session is found to be valid, the user is not prompted for login information because the existing session contains the information that the user has already been authenticated. However, different authorization rules are checked for privilege levels within the new application and passed along to the application, so that the user only gets access to authorized resources across multiple applications.

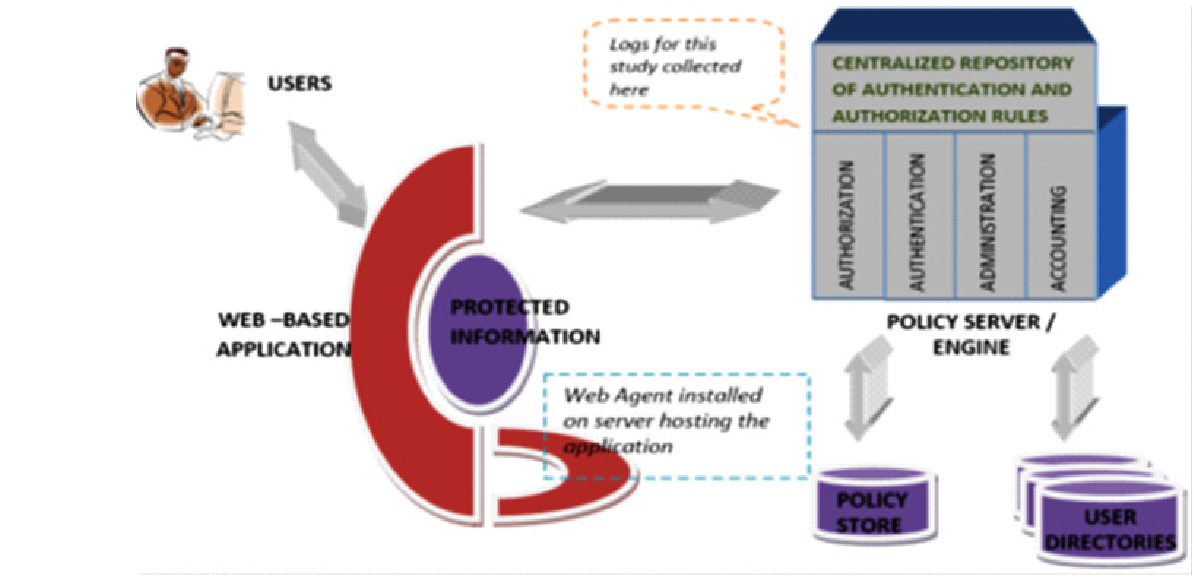

USERS
Logs for this study collected here
CENTRALIZED REPOSITORY OF AUTHENTICATION AND AUTHORIZATION RULES
AUTHORIZATION
AUTHENTICATION
ADMINISTRATION
ACCOUNTING
WEB -BASED APPLICATION
PROTECTED INFORMATION
POLICY SERVER / ENGINE
Web Agent installed on server hosting the application
POLICY STORE
USER DIRECTORIES

Figure A1. ESSO Architecture and Components

Appendix B

Mapping Application Characteristics to Routine Activity Theory Constructs: A Delphi Exercise

We carried out a Delphi-type exercise to understand and establish the connection between each application characteristic and routine activity theory constructs. The Delphi method is a commonly used research methodology for building and reporting consensus derived from initial divergent decisions and opinions by subject experts (Yoon 2011). To build consensus it requires an iterative process and anonymity of experts. The experts in our exercises were 13 application owners who were ultimately responsible for the security and risk management of their applications. These application owners had an average of 15 years of direct and relevant experience in managing applications and any associated risks. Their level of domain knowledge, which is the most important factor (Reb and Connolly 2009), would ensure the accuracy and validity of results.

Table B1. Application Characteristics and Routine Activity Theory Constructs

Variable	Application Characteristic	Routine Activity Theory Construct	Delphi 2nd Round Mean (STD)
BVM	Business Value Measure	Value	4.3 (0.48)
CSTR	Application Control Strength	Inertia	3.8 (0.63)
APL	Access Prevalence Level	Visibility	3.8 (2.10)
OLIM	On-demand Live Information Modification	Accessibility	3.9 (0.74)
DPL	Data Protection Level	Guardian	2.5 (2.64)

In the exercise, we asked the experts to identify routine activity theory construct(s) that would best connect to the application characteristics and also rate their confidence on an ordinal scale of 1 to 5 (1 being least confident to 5 being extremely confident). We performed two iterations of data collection. In the first round of data collection, we initially provided a brief primer on routine activity theory and application characteristics to each of the 13 experts (application owners) via e-mail. Then we followed up with a questionnaire to assign ratings for any routine activity theory construct with the application characteristics. We also solicited free-form comments and notes on their choices (which were suggested as optional). After receiving the completed questionnaires, during the second round of data collection, one author had about 30 minutes of telephonic conversation with each expert to explain the overall results regarding routine activity theory constructs and shared other participants' reasons of their selections. After this, the completed questionnaire was returned to each participant to revise their selections and ratings, if they wished to do so, based on the discussion about other participants' selections and comments. Ten experts returned usable results. We observed convergence in opinions of the experts in the second round of the study. Table B1 presents the mapping between an application characteristic and the routine activity theory construct to which it relates as well as the means and standard deviations of experts' ratings after the second round (on a scale of 1 to 5).

References

Reb, J., and Connolly, T. 2009. "Myopic Regret Avoidance: Feedback Avoidance and Learning in Repeated Decision Making," *Organizational Behavior and Human Decision Processes* (109:2), pp. 182-189.

Yoon, C. 2011. "Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model," *Journal of Business Ethics* (100:3), pp. 405-417.

Appendix C

Sample List of Application Controls

Access re-certification frequency

- A policy to specify the frequency for validation of users who have access to the application

Access to system controlled by enterprise web access management system

- This allows for secure and seamless provisioning, auditing and de-provisioning of user accounts

All deletions are marked for multiple approvals

- To mitigate against attempts to cover tracks and also to minimize accidental deletions

Annual audit of software business process

- Detailed auditing and testing of processes going through the application

Annual training on the system

- This is required for application users and their supervisors, reducing human errors

Application logs fed to SIEM system

- This allows for stronger and quicker detection of attempts of fraud, drawing events from across multiple applications

Approval and staging based version control system

- Several layers of approval and strict code migration policy

Automated fraud detection on select input screens

- Implementation of latest technology for analyzing screen inputs for potential fraud (based on correlation of other activities across other modules of same application or other interfacing applications)

Automated workflow of loan approval with connection with external third party systems to detect/investigate anomalies

- This allows for independent validation of loan-related decisions (often based on provided risk tolerance and other policies)

Common criteria–based software evaluation

- Extensive of standard accredited evaluations of deployed software

Complex password requirements

- Stronger and more complex requirements than other enterprise applications

Complies with policies associated with Internet-facing applications

- Much stricter policies for access and management of vulnerabilities

Continuous surveillance of shared machines that can be used for access to the financial information

- This allows for complete auditing of all the operations done on shared machines for select applications

Encryption of data in all stages except display

- Stronger security for data processed by the application

Enforced peer-review process to ensure integrity of BCP (Business Continuity plans)

- Each of these plans are reviewed through simulation by more than 3 independent peer groups

Enforcement of data segregation

- This is achieved through design of modules and screens; and application roles

Extensive documentation of use-policy and confidentiality disclosures

- This provides an important aspect of user/human-related risks

Financial-based controls for integrity and consistency checks

- This allows tiered and independent check of financial transactions

Group-based authorization

- These applications have authorization based on functional and business groups

Highly detailed functional and technical documentation

- The documentation is explicitly expanded to include much more information than is included in any standard package/implementation

Inbuilt escalation controls and process

- Automatic queuing of transactions for additional review and approval for certain transactions and processes

Job rotation

- Express application-based forced rotation for users belonging to specific roles per defined policies

Output management controls

- This limits the ways data/output can be shared and produced thereby limiting leak and steal

Part of operational risk oversight program

- This provides additional layers of closer scrutiny or design of application and ensuing operations on the application

Proprietary encryption for data manipulation and transmission

- This allows for security through obscurity and also keeps data secure

Real time monitoring of access attempts

- These applications have access logs fed to systems that are monitored in real time as opposed to just logging and collection at a central location

Results of monitoring and testing are maintained by the Compliance Department

- Reviews and audits are overseen by compliance in addition to usual groups

Second factor authentication for access to specified classification data

- Additional authentication enforced for access to higher classification of data

Strict server and file access limited to firewall procedure only

- Stronger access management and audit trail for access to data

Strict session controls

- This allows for tight monitoring of user's actions during a session (also across applications)

Stringent separation of duties through application role design

- Checks to ensure complete separation of duties per application roles and functions

Tighter change control within application

- Additional layers of change management for approval and execution

Use of FIPS (Federal Information Processing) standards for interfacing tools and utilities

- A control for stronger security over transactions and processing

Real-time backup of images offsite

- Strong mitigation against threats to availability of services and data

Reporting and exception tracking

- Transactions and processes outside of baselines are tracked and reported

Conciliation of vendor records with internal through monthly review process

- A control to reconcile financial numbers and transactions to detect anomalies

Quarterly penetration testing

- Technical vulnerability assessment of application

Code Review Controls

- Source code is reviewed on a regular basis, including every time a change is scheduled for implementation

Appendix D

Six Levels of Data Protection

The following describes the types of data and the required security protection for the five levels of data protections in the financial institutions used in the field study.

- Restricted (5): Information that is extremely sensitive and is intended for use only by select individuals within the company. Examples include personal identification numbers (PIN), PIN offsets, PIN generation keys (PGKs), credit or debit card data (Plastic Card #, ATM card #, etc.) (non-masked), card validation value or code (CAV, CVC, CVV, CSC, CID, CAV2, CVC2, CVV2 numbers, etc.), and "usable" encryption keys.

The following are the minimum security requirements for protection of the data: Encryption on such data is required for electronic storage and all non-trusted connections on public network transmissions. Access to the data is restricted through proper authentication. Physical transport of the data must be compliant with the ANSI approved ASC X9 standards or approval by the information security department. Such data cannot be sent using Internet e-mails or stored using portable media, nor can these data be published on intranet or external sources. Access to the data must be approved and authorized. A nonemployee must sign a nondisclosure agreement to access the data. Physical storage of the data must be in areas with restricted physical access.

- Private (4): Information that is intended for use on a need-to-know basis. Data are highly sensitive and are generally governed by governmental privacy laws and regulatory requirements. Examples include nonpublic personal consumer and/or commercial information (e.g., Social Security # (SSN), TIN #, or EIN #) (non-masked), commercial customers' data, financials, and information about their clients, personnel files, personal health information, merger/acquisition documentation, nonpublished financial information, wire transfer transactions.

  Different from Restricted (5) data on the minimum security requirements for protection of the data, encryption on such data is required only for all non-trusted connections on public network transmissions. If encrypted, such data may be sent using Internet e-mails or stored using portable media. Physical transport of the data may be carried out by employees, approved nonemployees, or other approved carriers. Access to such data must be approved and authorized. It can be published on an intranet with proper authentication mechanisms implemented, but not on external sources.

- Proprietary (3): Information is intended for use only by specified groups of employees because of its corporate/restrictive nature. Examples include account numbers, market analysis, budget information, operational risk data, and patents, trademarks, or trade secrets, confidential consumer and/or corporate information secured on the intranet (insider). The minimum security requirements for protection of the data are similar with those on Private (4).

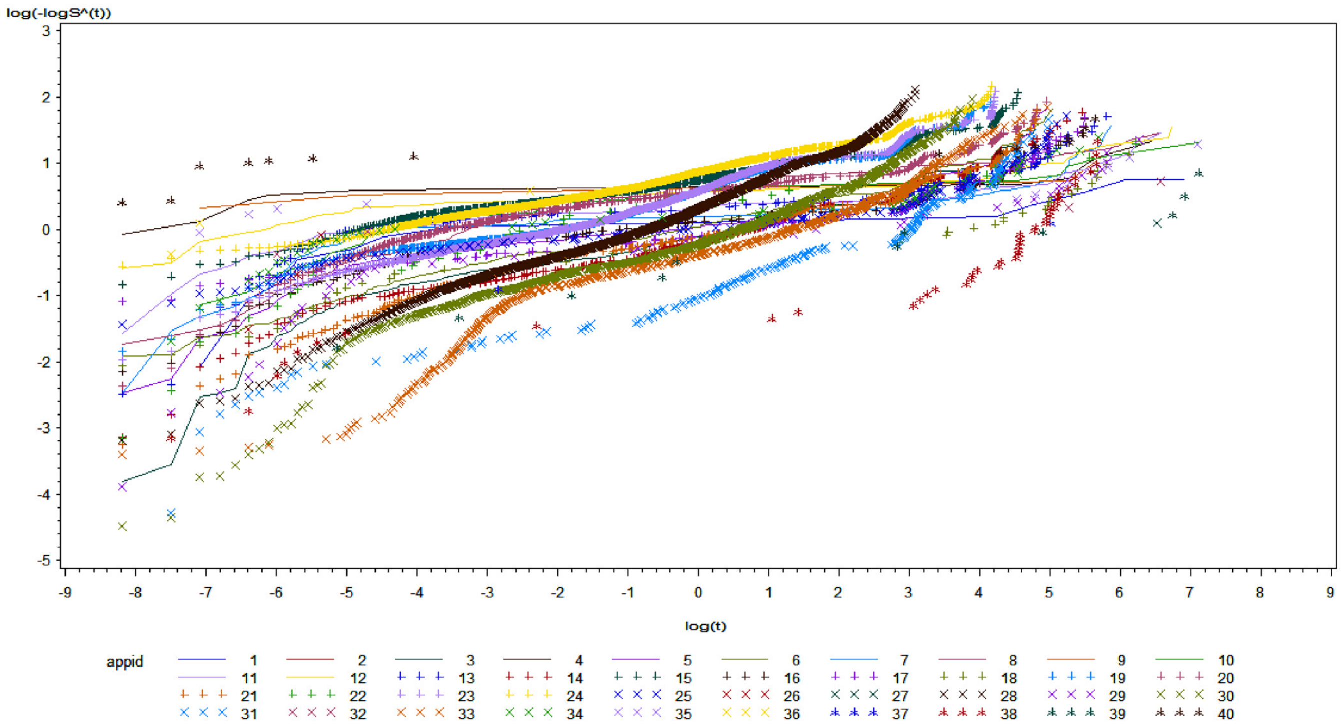
- Internal (2): Information that is available to all employees. Examples include asset tracking, internal communications, nonconfidential consumer and/or corporate information placed on the intranet (insider). Different from Proprietary (3) and Private (4) data on the minimum security requirements for protection of the data, encryption on such data is not required for electronic transmission and storage. Such data may be sent using Internet e-mails or stored using portable media without encryption. There is no authorization requirement on the access to such data. It can be published on an intranet with proper authentication mechanisms implemented as well as on external sources. Physical storage of the data can be in the possession of an employee or approved nonemployee.

- Public (1): Nonsensitive information that is available for general viewing (internal or external) because it is entirely nonsensitive. Examples include information in the public domain, approved press releases, approved marketing information, masked data with no other nonpublic personal consumer and/or commercial information (e.g., Social Security # (SSN), TIN #, or EIN #). There are no minimum security requirements for protection of the data.

- Not Applicable (0): Information that does not relate to any specific entity or operation. Examples include binary data logged at routers and dropped or lost network datagrams.

Appendix E

Plot of $\log\left\{-\log\hat{S}(t)\right\}$ Against log*t* for Different Applications


log(-logS^(t))
log(t)
appid