Financial assurance program for incidents induced by Internet-based attacks in the financial services industry

B. G. Raggad
Pace University, USA

Abstract

This paper furnishes an analytical model for the generation of a risk-driven financial assurance program capable of preventing, detecting, and responding to financial incidents (FAPG) for a general support system. Risk is defined in the paper as a basic belief assignment. The study reviews a single general support system with a known basic risk, integrating ids evidence and meta-evidence obtained from security management, in order to estimate the current system security risk position. The study shows the functioning of the FAPG, by generating a risk-driven financial assurance program, for a relatively small general support system in a firm in the financial services industry. This study is focused on financial incidents induced by Internet-based attacks but introduces a framework for further research.
Keywords: financial assurance, Internet, risk, security, World Wide Web.

1 Background

The story of financial fraud that affects consumers and firms is abundant in the literature. Forensic audits in general continue to indicate earnings overstated by millions if not billions of dollars in the United States. There is no doubt that corporate fraud in the United States has affected market values of firms, public pension funds, and consumer savings plans. Firms globally however continue to engage in a diversity of illegal and non-ethical accounting schemes. Effectiveness and timeliness of auditors in identifying fraud are of concern to industry internationally. It is important to discern what a firm can do if auditors fail to detect fraud. Is a computer information system capable of examining financial statements and detecting financial fraud? Efforts from investors and

WIT Transactions on Modelling and Simulation, Vol 43, © 2006 WIT Press
www.witpress.com, ISSN 1743-355X (on-line)
doi:10.2495/CF060051

auditors help in furnishing information critical in designing such a system and in clarifying the context of the financial statements and the content that may lead to early warning signs of earnings mismanagement.

In order to enable the feasibility of a fraud detection information system, the paper of this study posits a basic financial taxonomy as a framework for the design of this system. The organization of financial fraud generates an actual taxonomy based on the discrimination parameters of method of delivery, imposter, victim, and attack. The method of delivery has distinct values of phone, mail, media, and the e-Banking Internet. The imposter parameter has distinct values of user and business, and the victim parameter has similar values. The method of attack parameter has values of impersonation, decoy, information corruption, information leakage, and physical. This financial fraud taxonomy generates 4x2x2x5=80 classes of fraud. Sets of 80 fraud signatures can be applied in the design of the fraud detection information system. Fraud intrusion detection systems aim at detecting each of the 80 frauds, based on embedded information in signatures. Literature furnishes information on how to defend firms from the frauds and to implement countermeasures to preclude actualization of the frauds.

The study defines fraud response as the sequence of actions that are effected if a fraud is in action. That is, given the information of fraud responses, the study introduces an information system of detecting financial frauds, based on the aforementioned 80 signatures, and of enabling the planning of responses to preclude the detected fraud, search for the imposter, and recover from the prevented fraud. Such a system is defined effectively as a fraud detection and response system.

2 Introduction

A general support system is however interconnected information resources under the same direct management control which shares common functionality. This is the basic infrastructure of a financial firm owning e-Banking capabilities. A general support system normally includes hardware, software, information, data, applications, communication facilities, and personnel and furnishes support for a variety of clients and / or applications. A general support system, for example, can be a local area network, including smart terminals that support a branch office, an agency backbone, a communications network, or a departmental data processing center, including operating system and utilities. This study is focused on financial incidents induced by Internet-based attacks. The general support system is the only source of any network disruptions at the origin of financial incidents. A source of literature on Internet-based security disruptions is furnished in Ludovic and Cedric [1].

At the same time, institutions, including agencies of the federal government, have applications that have value and require protection. Certain applications, because of the information they contain, process or transmit, or because of their criticality to the missions of the institutions, require special management oversight. These applications are defined as major applications.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs, as for example, in an electronic funds transfer system. As in a general support system, a major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware / software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function, like an e-Banking application.

The function of a risk management program is to determine the level of protection currently provided, the level of protection required, and a cost-effective method of furnishing needed protection for a general support system of an institution or a major application. The output of such an activity is a risk-driven security program. The most fundamental element of risk management, in a financial firm, is however, the evaluation of the security position of the firm. Risk management identifies the impact of events on the security position and determines whether or not such impact is acceptable and, if not acceptable, furnishes corrective actions.

The primary purpose for conducting a risk analysis is to evaluate a system risk position of a firm and to identify the most cost-effective security controls for reducing risks. Risk analysis involves a detailed examination of the target system. It includes the threats that may exploit the vulnerabilities of the operating environment, which result in information leakage, information corruption, or denial of system services. Risk analysis activities are planned in terms of the current status and mission of the financial firm.

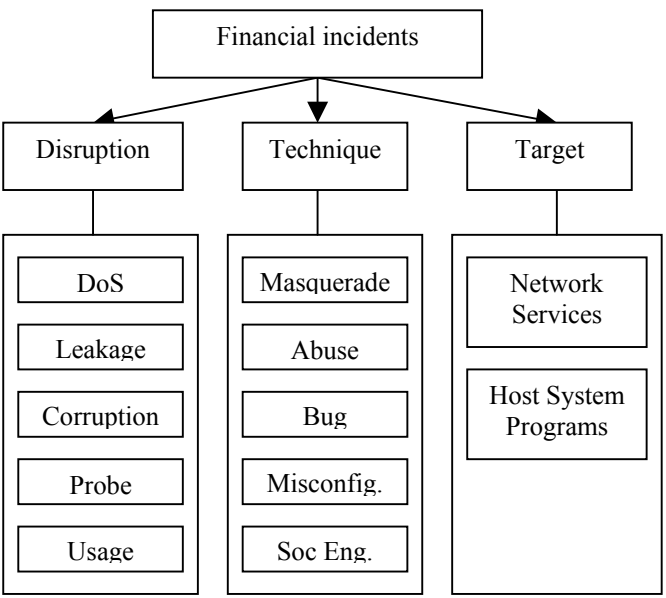

Figure 1: Threats to the general support system.

3 Methodology

The FAPG cycle organizes the evolution of the Internet-based attack steps that together generate additional risk to the target general support system of the firm or the major application. The target system starts by having vulnerabilities. If the target system does not suffer from any vulnerability conditions, then the system cannot be victim of attacks of attackers. Even if the vulnerability conditions exist but there are no threats capable of exploiting those conditions, then there will still be no risks to the target system. This study posits that the attacks are dormant until some vulnerability conditions and some exploiting threats co-exist in order for the attacks to be started by the attackers. Figure 1 furnishes a fundamental taxonomy of Internet-based attacks and techniques used to compose those attacks. Denning [2], Lippmann et al. Ludovic and Cedric [1] furnish further information on this taxonomy of attacks.

The passage from a dormant stage to an initiation stage may be achieved through the following access conditions, also defined as privilege conditions in Kendall [4]:

- IR: Initiation by Remote Access to Network;
- IL: Initiation by Local Access to Network;
- IP: Initiation by Physical Access to Host;
- IS: Initiation by Super User Account; and
- IU: Initiation by Local User Account.

The passage from the attack initiation stage to planning the attack involves the study and selection of the technique or model to be used in the attack process. As defined in Lippmann et al. e study is focused on the following attack models:

- PM: Planning Attack by Masquerade;
- PA: Planning Attack by Abuse;
- PB: Planning Attack by Exploiting a Bug;
- PC: Planning Attack by Exploiting an Existing Misconfiguration; and
- PS: Planning Attack by Social Engineering.

The passage from the planning stage to executing the attack may involve sequential steps, including testing or elevation of privileges to prepare the sufficient conditions to carry the attack. The taxonomy of attacks employed in designing the FAPG model is focused on the following attack classes:

- EP: Executing Attack by Probe;
- EL: Executing Attack by Information Leakage;
- EC: Executing Attack by Information Corruption;
- ED: Executing Attack by Denial of Service; and
- EU: Executing Attack by Unauthorized Use of Resources.

Figure 2 furnishes the steps needed to provoke some attack scenarios leading to financial incidents. The last stage in the FAPG cycle is the response stage. The appropriate response activities to mitigate risks generated following the execution of an attack are focused on the following classes:

- RM: Response by Managerial Controls;
- RO: Response by Operational Controls; and
- RT: Response by Technical Controls.

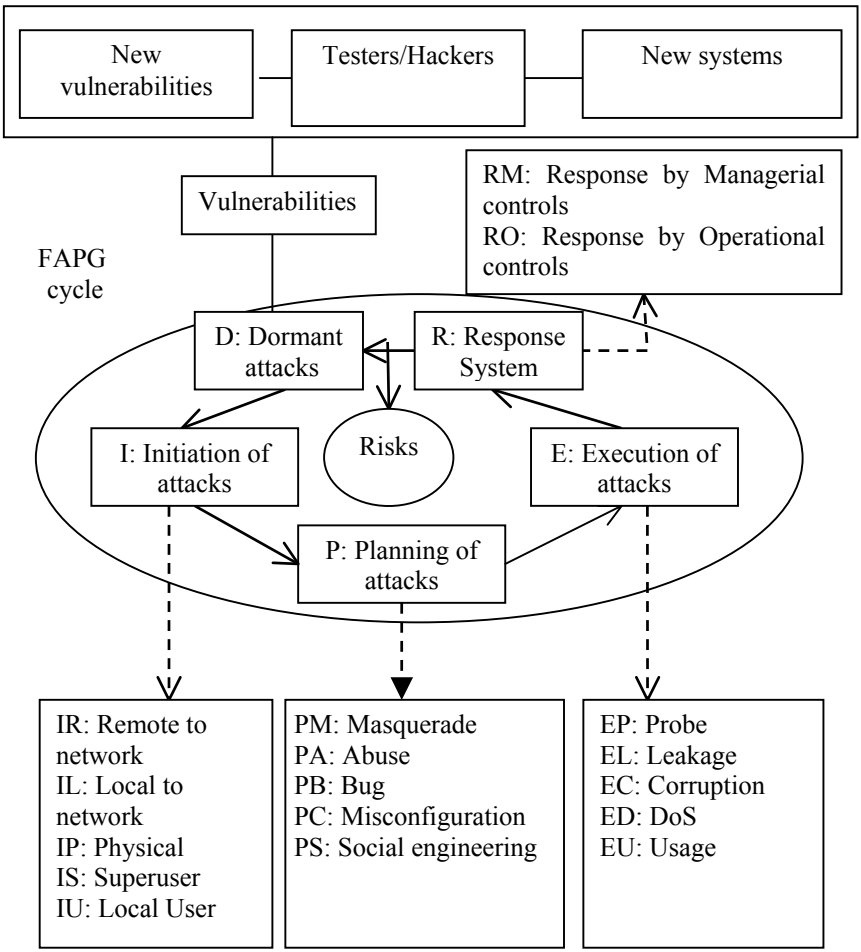

Figure 2: Attack initiation scenarios.

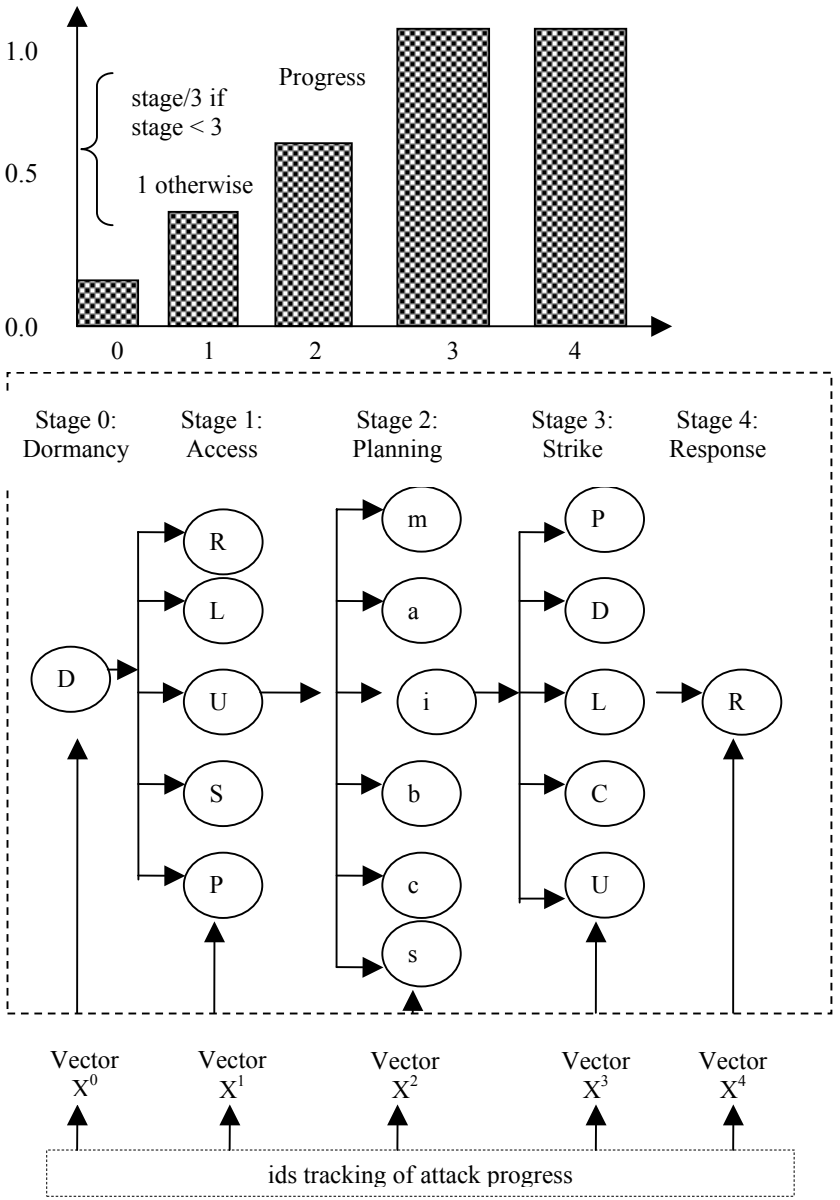

Figure 3: Detecting financial incidents through detecting security attacks.

4 Analysis

The FAPG captures all data describing the behavior of the general support system of the final institution and the major application, integrating simple log files or well-designed intrusion detection systems (ids) Denning [2] and Smets 5]. The system processes data to analyze all events that lead to financial incidents. Most often, the intrusion detection systems are sufficient to detect financial incidents and prevent the incidents Barrus [6], Porras and Neumann [7] and Ryon [8]. If these systems do not identify these attacks on time, then incident responses cannot be planned earlier to preempt the execution of those attacks. In this scenario, recovery actions are evoked by the firm. The study employed basic belief assignments (bba) to model the problem domain Smets 5], Smets and Kennes [9] and Lindqvist and Jonsson [10].

Assume that the basic risk is given by the following bba, where A denotes an attack and ┐A its negation:

$$m_0 \text{ bba on } \theta=\{A, \neg A\};\ m_0(A)=r_0;\ m_0(\theta)=1.$$

The current risk position of the firm is computed based on evidence obtained from the ids and meta-evidence obtained from the financial management team. Smets [5] and Smets and Kennes [9] further indicate belief functions in the modeling of uncertainty and generating decisions.

The ids generates the following evidence:

- $m^s[D]: 2^\theta$ [0, 1];
- $m^s[I]: 2^\theta \rightarrow [0, 1]$;
- $m^s[P]: 2^\theta \rightarrow [0, 1]$;
- $m^s[E]: 2^\theta \rightarrow [0, 1]$; and
- $m^s[R]: 2^\theta \rightarrow [0, 1]$.

Meta-evidence is defined in the following:

- $m^m[D]: 2^\theta \rightarrow [0, 1]$;
- $m^m[I]: 2^\theta \rightarrow [0, 1]$;
- $m^m[P]: 2^\theta \rightarrow [0, 1]$;
- $m^m[E]: 2^\theta \rightarrow [0, 1]$; and
- $m^m[R]: 2^\theta \rightarrow [0, 1]$.

The residual risks are computed in the following:

- $m^r[D] = m^s[D] \oplus m^m[D]$;
- $m^r[I] = m^s[I] \oplus m^m[I]$;
- $m^r[P] = m^s[P] \oplus m^m[P]$;
- $mr[E] = ms[E] \oplus mm[E]$; and
- $mr[R] = ms[R] \oplus mm[R]$.

The corporate security residual risk is computed in the following:

- $m^r = m^r[D] \oplus m^r[I] \oplus m^r[P] \oplus m^r[E] \oplus m^r[R]$.

That is, the system residual risk is expressed in the following:

- $m^r: 2^\theta \rightarrow [0, 1]$;
- $m^r(A) = m^r[D] \oplus m^r[I] \oplus m^r[P] \oplus m^r[E] \oplus m^r[R]$ (A); and
- $m^r(\theta) = 1 - m^r(A)$.

The response decision is illustrated in the decision tree furnished in Figure 3. The study assumes that risk owners at financial firms have their own private models that they apply in estimating financial recovery costs (R) and their own reservation values for their real losses (D), in the scenario of a given financial incident induced by an Internet-based attack.

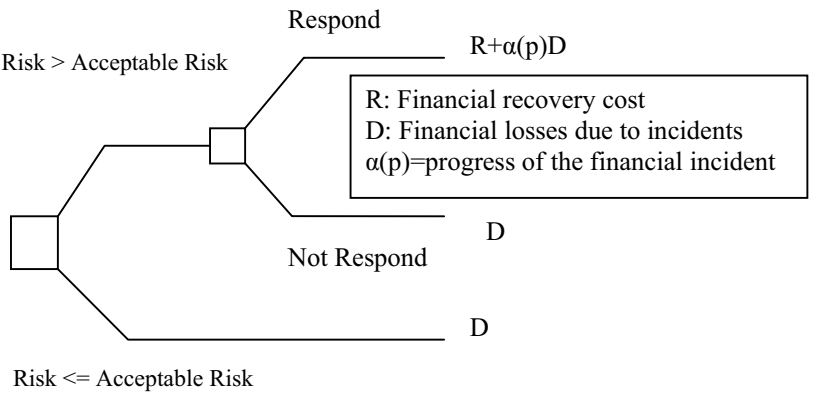

Figure 4: Responses to financial incidents based on risk.

5 Conclusion

This paper posited a new analytical model for the generation of a risk-driven financial assurance program capable of preventing, detecting, and responding to financial incidents (FAPG) for a general support system. The study reviewed a single general support system with known basic risk, integrating ids evidence and meta-evidence obtained from financial management, in order to estimate current financial risk positions. The study showed the functioning of the FAPG, by generating a risk-driven financial assurance program, for a small general support system in a financial firm. This study was limited to financial incidents induced by Internet-based attacks but introduced a framework for further innovation and research, which will be of interest to chief security officers in the financial services industry.

References

[1] Ludovic, M. & Cedric, M., Intrusion detection: a bibliography. *Technical Report* SSIR-2001-01, SUPELEC, France, September, 2001.

[2] Denning, D., *Information Warfare and Security*, Addison Wesley: Reading, MA, 1999.

[3] Lippmann, R. et al., Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation. *Proceedings of the 2000 DARPA Information Survivability Conference and Exposition*, January, 2000.

[4] Kendall, K., A database of computer attacks for the evaluation of intrusion detection systems. *Thesis, Master of Engineering in Electrical Engineering and Computer Science*, Massachusetts Institute of Technology, Boston, June, 1999.

[5] Smets, P. Belief functions: the disjunctive rule of combination and the generalized Bayesian theorem. *International Journal of Approximate Reasoning*, 9, pp. 1-35, 1993.

[6] Barrus, J., Intrusion detection in real time in a multi-node, multi-host environment. *Thesis, Master of Science*, Naval Postgraduate School, Monterey, CA, September, 1997.

[7] Porras P. & Neumann, P.G., EMERALD: event monitoring enabling responses to anomalous live disturbances. *Proceedings of the 20th National Information Systems Security Conference*, National Institute of Standards and Technology, October, pp. 353-365, 1997.

[8] Ryon, L.E., A method for classifying attack implementation based upon its primary objective. *Thesis, Master of Science*, Iowa State University, Ames, Iowa, 2004.

[9] Smets, P. & Kennes, R., The transferable belief model. *Artificial Intelligence*, 66, pp. 191-234, 1994.

[10] Lindqvist, U. & Jonsson, E., How to systematically classify computer security intrusions. *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, May, 1997.