Information Management Security in Multiple Networks For Development of Business and E-Commerce

Dinesh Kumar[1] and Kavita Dua[2]
[1]Research Scholar, NIMS University, Jaipur, India
[2]Associate Professor, OITM, Hisar
[1]dinesh.muwal@gmail.com

ABSTRACT: In this research paper we will discuss about Internet which has become the information super highway. The evolving Internet and its related technologies have allowed businesses to communicate in new and strategic ways with various types of people and organizations. Over the years, there have been additions of feature upon feature to the Internet connections. As the needs have changed, human beings have come across the need of more robust services, faster connections, and more flexibility in what can be done. In the beginning, services like simple POP3-style email and Web access were the extent of an Internet connection. Today we have site-to-site Virtual Private Networks (VPNs), client-side and home-user VPNs, streaming media, Web-based training, exciting Internet applications, e-commerce, and business-to-business extranets. Thus the Internet evolves towards fulfilling various advanced needs of human society.

Index Terms: Biometrics, Web services, vulnerabilities, e-commerce, WSDL, Infrastructure and Artificial intelligence

1. INTRODUCTION

First of all in introduction we will take a look about Information security management is the framework for ensuring the effectiveness of information security controls over information resources to ensure no repudiation, authenticity, confidentiality, integrity and availability of the information. Organizations need a systematic approach for information security management that addresses security consistently at every level. However, the security infrastructure of most organizations came about through necessity rather than planning, a reactive-based approach as opposed to a proactive approach[1]. Intrusion detection systems, firewalls, anti-virus software, virtual private networks, encryption and biometrics are security technologies in use today. Many devices and systems generate hundreds of events and report various problems or symptoms. Also, these devices may all come at different times and from different vendors, with different reporting and management capabilities and—perhaps worst of all—different update schedules. The security technologies are not integrated, and each technology provides the information in its own format and meaning. In addition, these systems across versions, product lines and vendors may provide little or no consistent characterization of events that represent the same symptom. Also, the systems are not efficient and scalable because they rely on human expertise to analyze periodically the data collected with all these systems. Network administrators regularly have to query different databases for new vulnerabilities and apply patches to their systems to avoid attacks. Quite often, different security staff is responsible and dedicated for the monitoring and analysis of data provided by a single system. Security staff does not periodically analyze the data and does not timely communicate analysis reports to other staff. The tools employed have very little impact on security prevention, because these systems lack the capability to generalize, learn and adapt in time.

Hence, the limitations of each security technology combined with attacks growth impact the efficiency of information security management and increase the activities to be performed by network administrators. Specific issues include data collection, data reduction, data normalization, event correlation, behavior classification, reporting and response.

Further, cyber security plans call for more specific requirements for computer and network security as well as emphasis on the availability of commercial automated auditing and reporting mechanisms and promotion of products for security assessments and threat management[2]. Recent initiatives to secure cyberspace are based on the introduction of cyber-security priorities that call for the establishment of information sharing and analysis centers. Sharing information via Web services brings benefits as well as risks (Dornan, 2003). Security must be considered at all points and for each user. End-to-end security is a horizontal process built on top of multiple network layers that may have security or no security. Security is a process based on interdisciplinary techniques (Mena, 2004; Maiwald, 2004).

2. REVIEW LITERATURE ON SECURITY THREATS IMPACT

Information security means protecting information and systems from security threats such as unauthorized access, use, disclosure, disruption, modification or destruction of information. The frequency of information security breaches is growing and common among most organizations. Internet connection is increasingly cited as a frequent point of attack and likely sources of attacks are independent hackers and disgruntled employees. Despite the existence of firewalls and intrusion detection systems, network administrators must decide how to protect systems from malicious attacks and inadvertent cascading failures. Effective management of information security requires understanding the processes of discovery and exploitation used for attacking. An attack is the act of exploiting a vulnerability that is a weakness or a problem in software (a bug in the source code or flaw in design). Software exploits follow a few patterns; one example is buffer overflow. An attack pattern is defined as a "blueprint for creating a kind of attack" (Hoglund & McGraw, 2004, p. 26). Buffer overflow attacks follow several standard patterns, but they may differ in timing, resources used, techniques and so forth.

Broad categories of attack patterns include network scanning, operating system stack identification, port scans, trace route and zone transfers, target components, choosing attack patterns, leveraging faults in the environment, using indirection and planting backdoors. Typically, an attack is a set of steps. The first phase is discovery or network reconnaissance. The attacker collects information about the target using public databases and documents as well as more invasive scanners and grabbers. Then, the attacker tries to discover vulnerabilities in the services identified, either through more research or by using a tool designed to determine if the service is susceptible. From a damage point of view, scans typically are harmless. Intrusion detection systems classify scans as low-level attacks because they don't harm servers or services. However, scans are precursors to attacks. If a port is discovered open, there is no guarantee that the attacker will not return, but it is more likely that he will and the attack phase begins. Several services and applications are targets for attack.
"Web within Web" [3] or Web services such as UDDI (finding a Web site), WSDL (site description), SOAP (transport protocol) and XML (data format) are security concerns. Much Web services security technology is still being developed and has not stabilized enough to inspire confidence. For example, protocols (SOAP) are lacking security, or specifications for Web services security (WS-SEC) are still evolving, and providing security in hardware is not an option because the specifications are not ready to be set in silicon (Dornan, 2003). On the other hand, standards themselves do not guarantee interoperability or security. It depends on how vendors implement the standards (Navas, 2002). Sometimes, Web security requires use of public key infrastructure (PKI). However, PKI is complex and has been a difficult infrastructure to manage, and the cost of managing has been detrimental to many organizations (Geer, 2003). Also, PKI infrastructure is not readily available in many parts of the world.

Spam is another threat that is increasing each year. The best anti-spam solutions rely on a set of detection methods such as heuristics, white and black lists, and signature matching. Choosing the right solution for an organization implies understanding how common spam filters operate, and what their tradeoffs are. Filtering the spam requires human intervention even when tools are available. Bayesian filtering promises a future where most of the spam could be detected and blocked automatically, but these tools are too complex for a mass audience, and wide-scale adoption is probably a few years out (Conry-Murray, 2003).

A very common threat is unauthorized access. This can be prevented via access controls enhanced with biometric systems, a type of access control mechanism used to verify an individual's identity. Biometric systems fall into two categories: authentication and identification, with authentication systems by far more common. Authentication systems are reliable and efficient if the subject base is small and the biometric readers are accurate and durable. A database with biometric data presents a natural target for theft and malicious and fraudulent use [4]Voice authorization products are becoming popular because they allow remote authentication , but the technology is the least accurate and network administrators have to use it cautiously until researchers improve it.

Moving data over back-end networks, remote locations, shared recovery centers and outsourced information technology facilities also expose information to threats (Hughes & Cole, 2003). The next section describes major trends in information security management.

3. METHODOLOGY

Surveys of security technologies indicate that most organizations use security technologies such as firewalls, anti-virus software, some kind of physical security to protect their computer and information assets or some measures of access control (). Technologies such as virtual private networks () and biometrics using a fingerprint are

predicted to grow very fast, and others are still emerging. The newest version of an intrusion detection system based on open-source Snort 2.0 supports a high-performance multi-pattern search engine with an anti-denial of service strategy [5]. However, detecting distributed denial-of-service (DDoS) is still emerging due to the complexity of technical problems not known to build defenses against this type of attack. Current technologies are not efficient for large-scale attacks, and comprehensive solutions should include attack prevention and preemption, attack detection and filtering, and attack source trace back and identification (Chang, 2002).

In addition, new protocols are defined and old protocols are enhanced. One example is IP security protocol (IPSec) defined by IETF. IPSec protocol is implemented for new IPv6 services in the very high-broadband-speed networks for new-generation Internet applications (Adam, Fillinger, Astic, Lahmadi & Brigant, 2004). In the near future, the network environment is expected to include hosts that support IPv4 and IPv6 protocols (Tatipamula, Grosette & Esaki, 2004), and new tools are needed for network administrators.

Other trends include integration of information security with physical security (Hamilton, 2003), self-securing devices and sensor networks. Self-securing devices offer new capabilities for dealing with intrusions, such as preventing undetectable tampering and deletion. If the detection mechanism discovers a change, an alert is sent to the network administrator for action (Cummings, 2002). Sensor networks are essential to the creation of smart spaces, which embed information technology in everyday home and work environments (Marculescu, Marculescu, Sungmee & Jayraman, 2003; Ashok & Agrawal, 2003). The privacy and security issues posed by sensor networks and sensor detectors represent a rich field of research problems (Chan & Perrig, 2003).

3.1 EMERGING SECURITY TECHNOLOGIES

Within the past years, a new security market has emerged, known as Security Event Management (SEM), which is part of Security Incident Management. SEM includes the processes that an organization uses to ensure the collection, security and analysis of security events as well as notification and response to security events. Although limited on capabilities, new products based on solutions for SEM are emerging slowly. The new products lack the prevention capability and still rely on human expertise to make decisions, or require substantial manual configurations up front. Data mining and other techniques for extracting coherent patterns of information from a call are near the top of the research agenda. For example, focusing on telephone calls from a particular installation, searching for specific words and phrases in e-mails, or using voice recognition techniques all are deployed. Cell and satellite phones can also reveal a caller's location (Wallich, 2003). The following section discusses issues and solutions for information security management.

4. SOLUTION OF INFORMATION SECURITY MANAGEMENT

IBM's manifesto (Kephart & Chess, 2003) points out difficulties in managing computing systems because their complexity is approaching the limits of human capability while there is need for increased interconnectivity and integration. Systems are becoming too complex for even the most skilled system integrators to install, configure, optimize and maintain. Information security management is no exception. One proposed solution is autonomic computing — computing systems that can manage themselves given high-level objectives from administrators. These systems require capabilities for self-configuration, self-optimization, self-healing and self-protection. Therefore, the success of autonomic computing is in the future, many years ahead.

In more sophisticated autonomic systems, machine learning by a single agent is not sufficient, and multi-agent solutions are proposed, although there are no guarantees of convergence because agents are adapting to one another. The agents change their behavior, making other agents change their behavior. Artificial intelligence (AI) techniques enhance agent capabilities. Intelligent agents and multi-agent systems are among the most growing areas of research and development. Intelligent agent technology is not a single, new technology, but rather the integrated application of technologies such as network, Internet and AI techniques. Learning in multi-agent systems is a challenging problem, so it is optimization. Intelligent models of large networked systems will let autonomic elements or systems detect or predict overall performance problems from a stream of sensor data from individual devices. At long time scales—during which the configuration of the system changes—new methods will be feasible to automate the aggregation of statistical variables to reduce the dimensionality of the problem to a size amenable to adaptive learning and optimization techniques that operate on shorter time scales.

Contrary to autonomous systems, new systems focus on human-agent effective interaction such that security policies can control agent execution and communicate with a human to ensure that agent behavior conforms to desired constraints and objectives of the security policies (Bradshaw, Cabri & Montanari, 2003; Bhatti, Bertino, Ghafoor & Joshi, 2004). A Microsoft project on next-generation secure-computing base is focused on building robust access control while retaining the openness of personal computers by providing mechanisms that allow operating systems and applications to protect themselves

against other software running on the same machine (England, Lampson, Manferdelli, Peinado & Williams, 2003). Still, robustness against software attacks will depend on hardware and software free from security relevant bugs. A business solution is to enforce quality security to software manufacturers and liability to the computer industry (Schneir, 2004).

Efficient information security management requires an SEM approach with enhanced real-time capabilities, adaptation and generalization to predict possible attacks and to support humans' actions. The following section discusses major requirements for the SEM model.

4.1 SEM MODEL REQUIREMENTS

The objective of the SEM is the real-time analysis and correlation of events. The model should be adaptable and capable to support monitoring and control of the network to include data collected by all security technologies and network management systems instead of relying on data provided by each single system. Although advanced techniques based on AI are emerging, these are still focused on a limited scope. For example, Sun Microsystems developed a host-based intrusion detection system using expert systems techniques for the Sun Solaris platform (Lidqvist & Porras, 2001). The SEM model should be cost effective such that organizations could afford the use of advanced technologies for security protection (Wallich, 2003).

The SEM model should be a hybrid model based on the integration of traditional statistical methods and various AI techniques to support a general system that operates automatically, adaptively and proactively (Hentea, 2003, 2004). Statistical methods have been used for building intrusion and fault detection models (Manikopoulos & Papavassiliou, 2002). AI techniques such as data mining, artificial neural networks, expert systems and knowledge discovery can be used for classification, detection and prediction of possible attacks or ongoing attacks. Machine learning technique is concerned with writing programs that can learn and adapt in real time. This means that the computer makes a prediction and then, based on the feedback as to whether it is correct, learns from this feedback. It learns through examples, domain knowledge and feedback. When a similar situation arises in the future, the feedback is used to make the same prediction.

The security model should include identification and selection of data needed to support useful feedback to a network administrator or security staff. In addition, the type of feedback available is important. Direct feedback entails specific information about the results and impact of each possible feedback. Indirect feedback is at a higher level, with no specific information about individual change or predictions but whether the learning program can propose new strategies and changes. Another important factor to consider is that systems, software and security policies change themselves over time and across different platforms and businesses. These special circumstances have to be included in the machine learning program to support the user and the security management process. In addition, the machine learning program should support a knowledge base to enrich the learning environment that allows the user to answer about unknowns in the system.

5. CONCLUSION

Security event management solutions are needed to integrate threat data from various security and network products to discard false alarms, correlate events from multiple sources and identify significant events to reduce unmanaged risks and improve operational security efficiency. There is a need for increased use of automated tools to predict the occurrence of security attacks. Auditing and intelligent reporting mechanisms must support security assessment and threat management at a larger scale and in correlation with the past, current and future events.

6. REFERENCES

[1] Gordon, Loeb & Lucyshyn, 2003, Iterative Enhancement: A Practical Technique for Software Development, IEEE and computer aided software engineering (CASE) tools Trans. Software Engineering, 1,4, 390-396, 1975.

[2] Hwang, Tzeng & Tsai, 2003; Chan, 2003; Leighton, 2004, Transformational Implementation: An Example, IEEE Trans. Software Engineering, 7, 1, 3-14, 1981.

[3] Castro-Leon, 2004, p. 42, Perspective on Automatic Programming, IEEE Trans. Software Engineering, 11,11,1257-1267, 1985.

[4] (Johnson, 2004, Vaughan-Nichols, 2004)., Understanding "why" in software process modeling, analysis, and design, Proc. 16th. International Conference of Software Engineering, 159 -168, 1994.

[5] (Norton & Roelker, 2003, Zeng & Ansari, 2003, Richardson, 2003), the Operational Versus the Conventional Approach to Software Development, Communications of the ACM, 27, 104-118, 1984.