Intelligent System for Information Security Management: Architecture and Design Issues

Mariana Hentea
Excelsior College, Albany, USA

Abstract

The limitations of each security technology combined with the growth of cyber attacks impact the efficiency of information security management and increase the activities to be performed by network administrators and security staff. Therefore, there is a need for the increase of automated auditing and intelligent reporting mechanisms for the cyber trust. Intelligent systems are emerging computing systems based on intelligent techniques that support continuous monitoring and controlling plant activities. Intelligence improves an individual's ability to make better decisions. This paper presents a proposed architecture of an Intelligent System for Information Security Management (ISISM). The objective of this system is to improve security management processes such as monitoring, controlling, and decision making with an effect size that is higher than an expert in security by providing mechanisms to enhance the active construction of knowledge about threats, policies, procedures, and risks. We focus on requirements and design issues for the basic components of the intelligent system.

Keywords: information security management, cyber security, intelligent system, architecture, agent-based control.

Cyber Security Overview

The exponential growth of the Internet, the convergence of Internet and wireless multimedia applications and services pose new security challenges (Miller, 2001). Security is a complex system (Volonino, 2004) and must be considered at all points and for each user. Organizations need a systematic approach for information security management that addresses security consistently at every level. They need systems that support optimal allocation of limited security resources on the basis of predicted risk rather than perceived vulnerabilities. However, the security infrastructure of most organizations came about through necessity rather than planning, a reactive-based approach such as detection of vulnerabilities and applying software updates (Cardoso & Freire, 2005) as opposed to a proactive approach (Gordon, Loeb & Lucyshyn, 2003). On the other hand, 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 (Chan & Perrig, 2003; Hwang, Tzeng & Tsai, 2003; Leighton, 2004).

Besides technical security controls (firewalls, passwords, intrusion detection, disaster recovery plans, etc.), security of an organization includes other issues that are typically process and people issues such as policies, training, habits, awareness, procedures, and a variety of other less technical and non-technical issues (Heimerl & Voight, 2005). Security education and awareness has been lagging behind the rapid and widespread use of the new digital infrastructure (Tassabehji, 2005). All these factors make security a process which is based on interdisciplinary techniques (Maiwald, 2004; Mena, 2004). The existing challenges of information security management combined with the lack of scientific understanding of organizations' behaviors call for better computational systems that support effectiveness of using specific information technologies and new approaches based on intelligent techniques and security informatics as means for coordination and information sharing. Intelligent systems emerged as new software systems to support complex applications. In this paper, we propose the architecture for an Intelligent System for Information Security Management (ISISM) which supports the security processes and infrastructure within an organization. Among these components, intelligent systems include intelligent agents that exhibit a high level of autonomy and function successfully in situations with a high level of uncertainty. The system supports knowledge acquisition that is likely to assist the human user, particularly at deeper levels of comprehension and problem solving for the information security assurance domain.

The next section of this paper provides a summary of information security management issues and trends, a brief overview of the information security threats, followed by a review of AI techniques for cyber security applications. Then we show the architecture and main components of the intelligent system and include specific design requirements for the intelligent agents. We discuss key issues related to design and technologies by using a Systems Engineering approach. We discuss that systems relying on intelligent agent-based control provide a way of analyzing, designing, and implementing complex software systems. We conclude with a perspective on the future of information security management efficiency and effectiveness by applying a multi-paradigm approach.

Information Security Management

Issues and Trends

Information security management is a framework for ensuring the effectiveness of information security controls over information resources. It addresses monitoring and control of security issues related to security policy compliance, technologies, and actions based on decisions made by a human. Information security management objective is to ensure no repudiation, authenticity, confidentiality, integrity, and availability of the information within an organization. Although different security technologies support specific security functions, there are many issues that impact the efficient management of information security. These technologies are not efficient and scalable because they rely on human expertise to periodically analyze the data. 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. These systems operating across versions, product lines, and vendors may provide little or no consistent characterization of events that represent the same symptom. These technologies lack features of aggregation and analysis of the data collected. In security management, analysts must choose how best to select observations, isolating aspects of interest. A static snapshot provided by one security technology (safeguard) does not provide the type of understanding needed for predictive analysis.

Organizations rely on human such as network administrator or security staff to regularly query different databases for new vulnerabilities and apply patches to their systems to avoid attacks.

Quite often, different security staff is responsible for the monitoring and analysis of data provided by a single system. Reports indicate that security staff does not periodically analyze the data and does not timely aggregate and communicate the results of the analysis reports to all parties involved with security management. Also, the tools employed have very little impact on security prevention because these systems lack the capability to generalize, learn, and adapt in time. Current security technologies lack the integration, prediction, and real-time feedback to humans to take measures to prevent or stop the attack. Also, the technologies are not efficient for large-scale attacks. In addition, the limitations of each security technology combined with the 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. To provide a complete, accurate, and comprehensive picture of network events that is desired by network administrators, a huge amount of event processing in near real-time, consolidation, and correlation of events are required.

Therefore, comprehensive solutions are needed to include attack detection and filtering, attack source trace back and identification, and attack prevention and preemption (Chang, 2002). There is a need for the increase of automated auditing and intelligent reporting mechanisms that support security assessment and threat management. Savely in his Prologue to Giarratano and Riley book said “the key to automation and our future lies in the effective application of the Computer Science field called Artificial Intelligence” (Giarratano & Riley, 1989). Solutions that support real-time analysis of threat data are very important because real-time detection allows security staff to prevent intrusions early in the attack cycle. This results in reducing the harm caused by successful attacks as well as decreasing the risks of losing the data and the need to perform recovery and extensive post-incident forensic analyses.

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 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. Unfortunately, successful autonomic computing is still in the future, many years away.

Contrary to autonomous systems, another trend is on systems focused on human-agent effective interaction. For example, 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 (Bhatti, Bertino, Ghafoor & Joshi, 2004; Bradshaw, Cabri & Montanari, 2003). 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 the unmanaged risks and improve the 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. The automated tools decrease the burden on human to process the significant data collected by different sources. Also, they reduce significantly the time to derive information from multiple systems and it will decrease the risk of missing possible attacks.

Efficient information security management requires a security event management approach with enhanced real-time capabilities, adaptation, and generalization to predict possible attacks and to support human’s actions. Dowd and McHenry (1998) point out that “network security must be better understood and embraced” and recommend strategies such as knowing the potential attacker, the value of protected assets, and understanding the sources of risk such as poorly administered system, social engineering, external or internal intrusion. To deliver protection against the latest generation of cyber threats, the rules of preemptive protection have to meet criteria for effectiveness, performance, and protection. Effectiveness of security management system is determined by the intelligence of the system, defined as the ability to detect unknown attacks with accuracy, along with enough time to strategically take action against intruders (Wang, 2005).

Information Security Threats

Information security threats are classified in two categories (Tassabehji, 2005):

- Technical sources such as intrusion attacks, probing or scanning, automated eavesdropping, automated password attacks, spoofing, denial of service attacks, and malware
- Non-technical such as natural disasters, physical infrastructure attacks, human error, and social engineering.

If organizations would have used an automated tool to analyze the network behavior, the damages caused by Slammer worm could have been greatly reduced or avoided in January 2003. The worm infected at least 75,000 hosts and caused interruption of business and daily activity (canceled airline flights, interference with elections, and failures of banks' automated teller machines) (Moore et al, 2003). The worm propagated very quickly from one network to another. The worm caused heavy traffic in the networks, bandwidth consumption, network equipment and database server failures due to resource exhaustion (CPU and memory), and internal DoS attacks including increased multi-casting traffic. If all these measurement trends were analyzed and correlations were performed by an intelligent tool, the damages caused by this worm could have been significantly reduced or avoided. Interpreting network traffic requires looking at many things and requires to logically analyze lots of data to draw an interpretation or conclusion in a short time.

Efficient management of information security requires understanding of the processes of discovery and exploitation used for attacking. 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 and network administrators ignore this information.

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. Despite the use of security technologies, network administrators must decide how to protect systems from malicious attacks and inadvertent cascading failures. One method called reconnaissance is used by hackers to choose networks and domains to search for targets. Reconnaissance allows a hacker to identify targets to be attacked or used for launching attacks. The targets are systems or networks with vulnerabilities. In order to protect against potential attackers, it is necessary to understand their reconnaissance methods and reasons. For example, by knowing the hacker's reconnaissance targets, network administrators and security staff can verify the targets and improve the security of the targets or the network. Therefore, monitoring and analysis of hacker's reconnaissance patterns has to be done correctly and continuously to determine the impact they may have on the security management. In supporting these activities, network administrators and security staff need automated and effective techniques for recognition and analysis of the reconnaissance patterns.

The following section discusses various applications based on different AI techniques for monitoring, control, and security applications.

Artificial Intelligence Techniques

AI techniques such as data mining, artificial neural networks, fuzzy logic, and expert systems can be integrated with traditional procedural and statistical methods to analyze the collected data by sensors, recognize reconnaissance patterns, filter and correlate events to support security event management and prevention of intrusions. These techniques improve the ability of security management systems to correlate events generated by a diversified suite of modern tools used for network management and security monitoring (Hentea, 2005a). Statistical methods have been used for building intrusion and fault detection models (Manikopoulos & Papavassiliou, 2002), but these models lack the capability to learn and adapt in time.

Expert systems are the most common form of AI applied today in manufacturing, telecommunications, business, and other areas. For example, Sun Microsystems developed a host-based intrusion detection system using expert systems techniques for Sun Solaris platform (Lindqvist & Porras, 2001). The systems, which are based on expert system and inference techniques, are not efficient and scalable because they mainly rely on human expertise, known facts and statistics implemented in rules for a specific host or network and their capability is limited. However, the expert systems evolved to a new trend of integration with the traditional information processing such that in the early nineties, the expert systems merged to a new infrastructure based on knowledge-based technology.

Knowledge-based systems, artificial neural networks, and fuzzy logic are the most promising approaches of AI for applications such as faults and events monitoring, detection, isolation, diagnosis, supervisory and adaptive control, direct control (Rodd, 1992). Adaptive control refers to the capability of the system to adjust (adapt) itself to meet a desired output despite shifting control objectives and process conditions or unmodeled uncertainties in process dynamics. The techniques associated with intelligent control include fuzzy, expert, and neural control (Hentea, 1997; Passino & Ozguner, 1996). Intelligent systems were developed for manufacturing automation at Ford Motor Company (Rychtyckyj, 2005).

Artificial Intelligence techniques enhance agent capabilities. Intelligent agents and multi-agent systems are among the most rapidly growing areas of research and development. Vulnerability assessment and intrusion detection based on agent approach are discussed in (Cardoso & Freire, 2005). Multi-agent framework design and implementation issues for the autonomous database administration system and security are described in (Ramanujan & Capretez, 2005). Strategies for security information analysis and data mining techniques to discover hidden information about possible cyber threats are discussed in (Yao, Wang, Zeng & Wang, 2005).

A multi-agent system is designed and implemented as several interacting agents. Multi-agent systems are ideally suited to representing problems that have multiple problem solving methods and multiple perspectives. Intelligent agents take initiative where appropriate, and socially interact, where appropriate, with other artificial agents and humans in order to complete their own problem solving and to help others with their activities.

Although techniques based on AI are emerging to support information security management, these are still focused on a limited scope. Recently, AI methods to create robust intrusion detection and prevention systems have been explored. Several techniques and examples of applications for intrusion detection and prevention systems are discussed in (Hentea, 2005b). Intelligent systems for network management support functions such as monitoring, diagnosing, or managing specific network resources are discussed in (Berenji, 1994; Hentea, 1999; Turban, Aronson & Liang, 2005). For example, WatchGuard software includes an intelligent agent that supports limited capabilities for firewall configuration management (http://www.watchguard.com). Artificial neural networks techniques are suggested for biometric identification applications (Kung, Mak &

Lin, 2005). A system based on neural networks agent for mail server management is discussed in Willow (2005).

AI techniques can be used in building intelligent models to improve the information security management, intrusion detection and prevention capabilities, efficiency of security event management, and decision making (Hentea, 2003, 2004, 2005b, 2005c). Intelligent systems called intelligent assistants help users in decision-making process for configuring and monitoring specific metrics, faults and events correlation that could lead to the reconnaissance of the attack and prevention of the cyber attack. Efficient information security management requires an intelligent system that supports security event management approach with enhanced real-time capabilities, adaptation, and generalization to predict possible attacks and to support human's actions. The following section describes the basic components and main functions of the intelligent system for information security management (ISISM).

ISISM Architecture

Any intelligent system consists of two parts (Meystel & Albus, 2002):

1. Internal, or computational, which can be decomposed into four internal subsystems of intelligence as follows:
   a) Sensory processing - inputs to an intelligent systems are provided via sensors and processed to create a consistent state of the world. Sensors are used to monitor the state of the external world and intelligent system itself.
   b) World modeling - is the estimate of the state of the world; it includes knowledge databases about the world and contains a simulation module that provides information about future states of the world.
   c) Behavior generation – is the decision making module that selects goals and plans, and executes tasks.
   d) Value judgment – it evaluates both the observed state and predicted state; it provides the basis for decision making.
2. External, or interfacing; input and output from the internal part of the intelligent systems are generalized via sensors and actuators that can be considered external parts.

In all intelligent systems, a sensory processing subsystem processes data from sensors to acquire and maintain an internal model (representation) of the world. Then, a behavior generating subsystem decides the course of actions to be taken for achieving the goal. The behavior generation subsystem controls actuators to pursue behavioral goals in the context of the perceived world model. Outputs from intelligent systems generate commands or actions to control the target system. Sensors data are the basis to build knowledge bases, derive new knowledge, detect and predict cyber attacks, and make timely decisions. Examples of sensors data include measurements related to performance, security, state for the following:

- Device such as CPU performance, memory usage, used disk space, file usage number of active connections, number of open connections, number of failed logins, number of transactions (queries, updates, deletion), new user requests, new software requests, user termination, response time, number of privileged users accessing the system at one time, number of concurrent users, configuration changes, file accesses per user, number of system calls, number of alerts, number of user authentication failures, number of pending connections, timeout periods, programs execution time, system files usage, shared library usage, clock synchronization protocols, system clock, user accesses to data and executable files, log files size, etc.

- Network such as available bandwidth, delay, network access requests, number of resources not available for some time, new protocol requests, number of simultaneous open ports, number of simultaneous transactions over the Internet, number of simultaneous transactions over the Intranet, configuration changes, excessive noise on a circuit requiring retransmission, number of packets dropped, number of E-mail messages, number of console messages, protocols usage, etc.
- Interfaces such as utilization statistics
- Environmental (temperatures, doors open, doors locked, alarms)
- Security safeguards (firewalls, intrusion detection systems, anti-virus software, virtual private network, encryption) such as: number of denied connections, number of alerts, number of false positives, number of false negatives, downtime, maintenance time, number of software updates, reconnaissance activities, number of encrypted and decrypted keys, remote accesses, etc.
- Security policies (issue date, revised date, targets, etc.)
- Risks (accepted, reduced, transferred)
- Contingency and recovery plans
- Security and network administrators activities (logins, configuration changes, software installed, software updates, testing, number of notification messages, user applications executed, etc.).

We adapt the system architecture referenced in (Meystel & Abus, 2002) which is based on the real control system (RCS) techniques. Meystel & Albus (2002, p. 19) mention that "intelligence in systems is created by a definite architecture that organizes joint functioning of otherwise non-intelligent devices". All elements of intelligence are based on elementary functioning loop (self containing agent) which allows to create functional relationships and information flows. Figure 1 shows the basic components of a self-containing agent for security. The cyber security of an enterprise is observed and/or controlled, or it serves as a medium for elementary functioning loop activities.

The agent has percepts (entered through sensors) as its inputs, and actions as its outputs (produced by effectors, called actuators). Software agents are computational units that are repeated many times within an intelligent system at many different levels as the units of information in all of the subsystems are aggregated into entities, events, situations, and goals are decomposed into subgoal tasks and generate actions or commands. Within each loop, security sensors processing and security modeling maintain a knowledge database with a characteristic range and resolution. At each level, plans are made and updated with different planning horizons. At each level, short-term memory traces sensory data over different historical data intervals. At each level, feedback control loops have a characteristic. For example, the controlled variables could be the bandwidth and latency of the network. This model of a multi-resolutional hierarchy of computational loops yields deep insights into the phenomena of behavior, perception, cognition, problem solving, and learning.

The architecture of an intelligent system is a specific framework of agents and each agent has its own architecture. In the core of any intelligent system, is also the concept of generalized agent. Agents with similar functions can be gradually lumped in a group type agent which is a generalized agent. The group agent gives a new world representation (or new granulation or new resolution). Further, group agents can be aggeregated into an even more generalized agent (group of groups agent) in a hierarchical structure. This architecture supports the model of information security management.

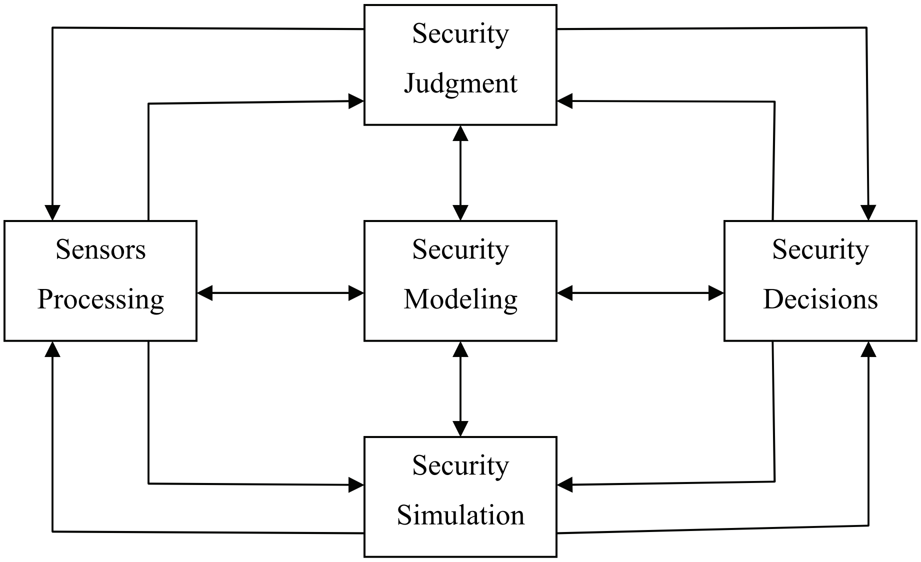

Figure 1: Self-containing agent, adapted from (Meystel & Albus, 2002)

Software agents that can change their location in the system are called mobile agents. Mobile agents can move across a network, and perform tasks on other machines. This allows processes to migrate from computer to computer and to return to their point of origin. Also, process migration allows executable code to travel and interact with databases, file systems, information services, and other agents. Mobile agents are used for network services discovery on live manets (mobile adhoc networks) environments (Kopena et al, 2005). Intelligent spaces based on intelligent devices are becoming common applications in smart homes, workplaces, classrooms, hospitals, and transportation services (Yang & Wang, 2005).

The proposed architecture includes elements of intelligence to create functional relationships and information flow between different subsystems. The elements of intelligence are based on components using one or more AI techniques: natural language processing, artificial neural networks, fuzzy logic. In addition, we see an advantage in the development of intelligent system of combining AI techniques with other techniques such as conventional programming and statistical packages creating a hybrid intelligent system architecture (Zahedi, 1993).

Figure 2 depicts the proposed architecture of the intelligent assistant system based on the integration of traditional statistical methods and various AI techniques to support a general system that operates automatically, adaptively, and proactively.

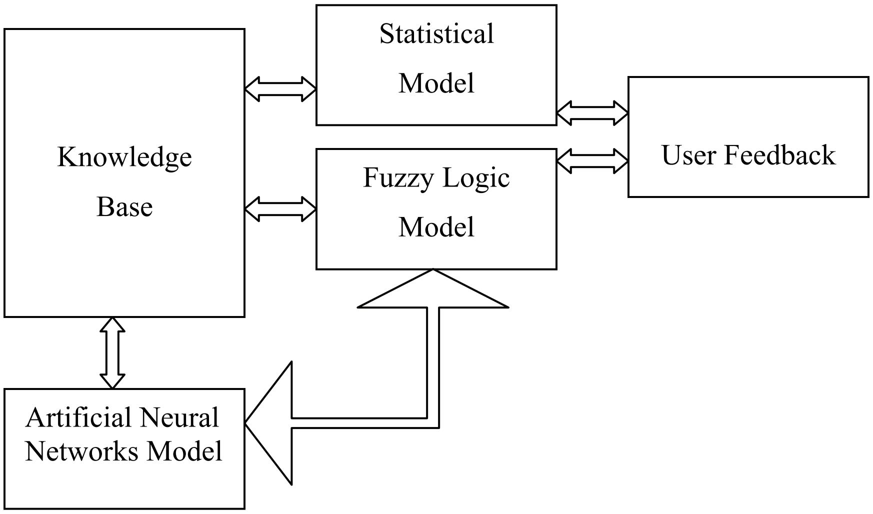

Figure 2: Intelligent Model Components

The system's architecture is based on a hybrid approach that yields both the robustness and depth of understanding of decision making using intelligent models. This system aims to improve monitoring and decision making processes with an effect size that is higher than an expert in security. In addition, this system provides mechanisms to enhance the active construction of knowledge about threats, policies, procedures, and risks. The model is adaptive and supports processing and classification of events and data that leads to the prediction of attacks. Any activity occurrence can be considered an event, from running the virus scan program to logging into a device.

One major component in design is the development of an intelligent model for the analysis and correlation of events and data in real-time to increase the detection and prevention capabilities of the security technologies: intrusion detection systems, firewalls, anti-virus software, spam filters, vulnerability assessment systems, etc. For example, neural and fuzzy models should be adaptive and support processing and classification of events and data that leads to the prediction of attacks as well as advice to the user via user feedback interface. Also, the fuzzy logic model supports risk management, a critical phase in the life cycle of the information security management (Hentea, 2006). The models should also be expanded to include input from the security plans and measures for network monitoring, auditing, physical and logical access controls. The models should support tasks for information security management such as monitoring, detection, identification of the threats as well as preventing the attack by taking preemptive actions when it is necessary, providing useful information about ongoing attack, and predicting possible attacks.

The results of sensing are encoded, filtered, and processed within sensor processing component, and submitted to the other components of self-containing agent (elementary functioning loop) depicted in Figure 1. Any component of elementary functioning loop may include one or more models of Figure 2. Data is passed to security modeling, security simulation, or behavior generator components that organize, classify, combine and correlate data, or generate new knowledge that is stored in the knowledge base.

The hybrid system is an integration of different models for the adaptive security event management to include AI techniques and other methods based on statistical and traditional procedural approach. The basic idea of the multiple models is to perform independently different functions with different measures, and to complement the weaknesses of one model with the strengths of another model. For example, artificial neural networks can be used to classify the reconnaissance patterns, but outputs or parameters can be presented to a fuzzy logic expert system that can interpret the data for human. Because the outputs of the models are uncertain and imprecise in some situation, and human experts can have some intuition or knowledge on the characteristics of the presented information, a fuzzy logic expert model could improve the outcomes of artificial neural networks model or just interpret the outcomes of other models in a form that humans relate better. In addition, fuzzy logic model can be used to learn fuzzy rules when there is no a priori knowledge about the fuzzy rules and fuzzy sets.

The model is based on agent technology to monitor, detect, and identify the threats as well as preventing the attack by providing useful information before an attack occurred. Agent-based applications have been used in manufacturing, process control, telecommunication systems, air traffic control, traffic and transportation management, information filtering and gathering, electronic commerce, business process management, entertainment and medical care (Jennings, Sycara & Wooldridge, 1998). Wang (2005) discusses intelligent agent-based control to network traffic management systems and transportation systems.

The system should include functions for automated tasks such as data collection, data reduction, filtering, and event correlation based on multi-agent technologies. The intelligent agents support information security measurements, monitoring, analysis, and control. The system may generate commands to end processes or move the processing to another device when signs of suspicious behavior or failures are detected. Devi & Ramachandran (2002) describe a multi-agent system for network management where agents negotiate the performance of the processors in the clustered network when service performances are downgraded..

In addition, our system is an intelligent assistant to provide user feedback such as help on making decisions and taking actions. In addition, the system should include a user interface based on multimedia for supporting network administrator's operations, and a knowledge base for maintaining trustworthiness as systems change and adapt. This knowledge base must be adaptive and shared via web. The validation of the computer generated decisions can be performed by comparing with the decisions of experts. In addition to automated methods for knowledge discovery, this method allows building knowledge base for decision making and taking actions using human experience and judgment.

The user feedback module should provide different feedback to a network administrator or security staff. 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. This is an important aspect of machine learning. Much of the machine learning research has focused on the learning portion rather than on creation of the feedback as useful information for the user to make decisions. The objective of the Intelligent System is on developing learning techniques that can support the business and advice the user to make decisions before the attack damaged the information or made the systems unavailable. Another important factor to consider is that systems and security policies change themselves over time and across the different platforms and businesses. These special circumstances have to be easily and timely included in the machine learning program to support the user. In addition, the machine learning program should support a knowledge base to enrich the learning environment.

Design Issues

A major decision to be made during the architectural design is what agents should be included. Several types of agents can be designed to support information security management (Russell & Norvig, 2003). In the proposed system, key agents should be the decision maker agent and controller agent.

An intelligent agent is viewed as a combination of functionalities and intelligent capabilities (ability to act in an uncertain environment, learning, adaptability, probability of success). Functionalities (called roles in some methodologies) are things the agents that will perform by looking at combinations of functionalities. Although there has been much debate on what constitutes an agent, and which features are important, the consensus is that an intelligent agent is situated, autonomous, reactive, proactive, and social. The main contributor to the field of autonomous agents is artificial intelligence.

Due to the complexity of information security management tasks, the proposed system is based on the integration of different types of intelligent agents, a hybrid architecture under real-time constraints. Intelligent agents help in automating various tasks such as gathering information, filtering, and using it for decision support and can help to improve the productivity of the network administrator. The design and programming of agents should be focused on maximizing their performance measure which embodies the criterion for success of an agent's behavior (Russell & Norvig, 2003). Other important issues that are required include portability, stability, resilience, and security of the agents and system (Bradshaw et al, 2001; Hamidi & Mohammadi, 2006). The interface should exhibit intelligent features that assist the user in decision making and taking actions to control the security process.

The performance measures should be designed according to what is needed in the environment of the information security management rather than according to how one thinks the agent should behave. In addition, the design phase has to identify the type of feedback available for learning because it is usually the most important factor in determining the nature of the learning problem that the agent faces. The field of machine learning usually distinguishes cases of supervised and unsupervised learning. The scope of managing information security is broad and requires using a single or a combination of both forms for getting the best results. Another characteristic that should be considered is the mobility which is the degree to which the agents travel through the network.

In addition, the representation of the data (inputs to the models for learning and outputs of the models) plays an important role in the design. Another factor in the design will consider the availability of prior knowledge for some tasks of information security management. The majority of learning will begin with no knowledge at all about what the agent is trying to learn. Learning takes place as the agent observes its interactions with the environment and its own decision-making processes. Learning is a process of self improvement and thus an important feature of intelligent behaviors.

The functions performed by each component can be developed based on the spiral development method. The suite of ISISM capabilities are based on the security requirements of each organization. The order of implementation of the models is dependent on the resources and needs. The following is a brief description of features as they were developed and used in different projects:

- Data mining supports automated analysis and interpretations of the data and events collected from different sources as well as discovery of associations among data and events and feedback to human user. Examples of use of data mining techniques and knowledge discovery are discussed in (Hentea, 2004; Ibrahim, Folorunso & Ajayi, 2005)

- Artificial neural networks support classification, association, and prediction of future cyber attacks by learning and adapting from past and current data and events. For example, reconnaissance patterns can be classified using neural networks based on unsupervised learning (Hentea, 2005b, 2005c)

- Fuzzy logic allows processing of qualitative variables and approximate reasoning when the propositions are inexact and vague. One model is used for risk assessment (Hentea, 2006)
- Intelligent assistance and user feedback techniques are discussed in (Hentea, 1997)
- Statistical approaches are discussed in (Hentea, 1997, 2006).

However, a synergy between different approaches can serve to enhance and highlight the qualitative aspects of each model, thus creating knowledge and intelligence for assisting the human to make decisions. A possible avenue for integrating data mining, neural networks, and fuzzy expert systems in addressing the intrusion attempts would be to use the data mining and neural network to discover and to classify the reconnaissance patterns and its attributes. This information can be communicated to fuzzy expert system that could then return advice to human to take actions based on the status of intrusion attempts. Further, neural networks can recognize patterns and predict possible cyber attacks. Also, neural networks can draw conclusions from fuzzy or uncertain data about a given situation. The knowledge-base incorporates knowledge for the security domain such as raw data and events, performance measures, patterns, policies, and decisions. In addition, knowledge refinement, knowledge representation, and knowledge discovery are essential components in a knowledge management system. Another requirement is the cost of development and maintenance. The system should be cost effective such that organizations could afford the use of advanced technologies (data mining, artificial neural networks, fuzzy logic, and knowledge base) for security protection and prevention (Wallich, 2003). Although we described several capabilities for the system, we did not provide an exhausted list of requirements. The intent of this paper is to provide a framework for designing an intelligent system for information security management. Similar intelligent systems for manufacturing are described in (ISAM, 2007).

Conclusion

Advanced real-time techniques based on modeling, sensor analysis, and intelligent agents integrated with traditional procedural and statistical methods can recognize, filter, and correlate events and data collected by various sensors and sources. These techniques support the capability to provide automated feedback to correct the problems including useful advice to a human to take actions and prevent ongoing attacks. We propose a novel architecture of an intelligent system for information security management. The proposed architecture is based on multidisciplinary paradigm which includes information security management, network communications, automata (process control), computer science, artificial intelligence, modern control theory, statistics, social sciences, organizational theory and behaviors, management science, business strategies, risk analysis, and economics. No single approach can resolve the growth and increased sophistication of cyber threats (Gordon, Loeb & Lucyshyn, 2006). We need to apply several paradigms to meet the objectives of information security management for the modern organization of the 21st-century. Based on foundational work in AI and other areas, intelligent agent technology has significant application in cyber security. Intelligent agent technology is considered by some researchers to be a natural successor of object oriented programming. No prototypes or systems of this kind have been identified. However, prototypes of isolated features or components are emerging, but these components require deeper development and integration. The system has to be adaptive and capable of discovering and building new knowledge for the information security domain. Future work should seek a systematic proof-of-concept that integrates all modules to support the security management.

References

Berenji, H.R. (1994). The unique strength of fuzzy logic control. *IEEE Expert*, *9* (4), 4.

Bhatti, R., Bertino, E., Ghafoor, A., & Joshi, J.B.D. (2004). XML-based specification for web services document security. *IEEE Computer*, *37* (4), 41-49.

Bradshaw, J.M., Suri, N., Canas, A.J., Davis, R., Ford, K., Hoffman, R., Jeffers, R., & Reichherzer, T. (2001).Terraforming cyberspace. *Computer, 34* (7), 48-56.

Bradshaw, J. M. Cabri, J., & Montanari, R. (2003). Taking back cyberspace. *IEEE Computer*, *36* (7), 89-92.

Cardoso, R.C. & Freire, M.M. (2005). Security vulnerabilities and exposures in internet systems and services. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking* (pp. 910-916). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Chan, H. & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer*, *36* (10), 103-105.

Chang, R.K.C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine*, *40* (10), 42-51.

Devi, S.S.E. & Ramachandran, V. (2002). Agent based control for embedded applications. Retrieved December 16, 2006, from http://www.hipc.org/hipc2002/2002Posters/AgentControl.pdf

Dowd, P.W. & McHenry, J.T. (1998). Network security: it's time to take it seriously. *IEEE Computer*, *31* (9), 24-28.

Giarratano, J. & Riley, G. (1989). *Expert systems principles and programming*. Boston, Massachusetts, PWS-KENT Publishing Co.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, *XIX* (2), 1-7.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2006). Computer and cyber security breaches: Schumpeter to the rescue. *Computer Security Journal*, *XXII* (4), 9-10.

Hamidi, H., & Mohammadi, K. (2006). Modeling fault tolerant and secure mobile agent execution in distributed systems. *International Journal of Intelligent Information Technologies*, *2* (1), 21-36.

Heimerl, J.L. & Voight, H. (2005). Measurement: The foundation of security program design and management. *Computer Security Journal*, *XXI* (2), 1-20.

Hentea, M. (1997). Architecture and design issues in a hybrid knowledge-based expert system for intelligent quality control. PhD Thesis, Illinois Institute of Technology, Chicago, Illinois.

Hentea, M. (1999). Intelligent approach for network management system: Architecture and design issues for ATM computer networks. *Proceedings of 1999 Advanced Simulation Technologies Conference*, San Diego, California.

Hentea, M. (2003). Intelligent model for cyber attack detection and prevention. *Proceedings of the ISCA 12th International Conference Intelligent and Adaptive Systems and Software Engineering*, San Francisco, California, 5-10.

Hentea, M. (2004). Data mining descriptive model for intrusion detection systems. *Proceedings of the 2004 Information Resources Management Association International Conference,* New Orleans, Louisiana, 1118-1119.

Hentea, M. (2005a). Information security management. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking (*pp. 390-395). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Hentea, M. (2005b). Improving intrusion awareness with a neural network classifier. *Proceedings of the ISCA 14th International Conference Intelligent and Adaptive Systems and Software Engineering*, Toronto, Canada, 163-168.

Hentea, M. (2005c). Use of reconnaissance patterns for intelligent monitoring model. *Proceedings of the 2005 Information Resources Management Association International Conference*, San Diego, California, 160-163.

Hentea, M. (2006). Enhancing information security risk management with a fuzzy model. *Proceedings of 19th International Conference on Computer Applications in Industry and Engineering*, Las Vegas, Nevada, 132-139.

Hwang, M3-S. Tzeng, S-F. & Tsai, C-S. (2003). A new secure generalization of threshold signature scheme. *Proceedings of International Technology for Research and Education*, 282-285.

Ibrahim, S.A., Folorunso, O. & Ajayi, O.B. (2005). Knowledge discovery of closed frequent calling patterns in a telecommunication database. *Proceedings of the 2005 Informing Science and IT Education Joint Conference,* Flagstaff, Arizona, 137-148. Available at http://proceedings.informingscience.org/InSITE2005/P13f80Ibra.pdf

ISAM. (2007). An intelligent systems architecture for manufacturing (ISAM): A reference model architecture for intelligent manufacturing systems**.** Retrieved January 15, 2007, from http://www.isd.mel.nist.gov/projects/rcs/isam/ISAM_web.htm#framework

Jennings, N.R., Sycara, K. & Wooldridge, M. (1998). A roadmap of agent research and development. In N. Jennings, K. Sycara, M. Georgeff (Eds.), *Autonomous Agents and Multi-Agent Systems, 1* (1), pp. 7-38. Boston, Massachussetts, Kluver Academic Publishers.

Kephart, J.O. & Chess, D.M. (2003). The vision of automatic computing. *IEEE Computer*, *36* (1), 41-50.

Kopena, J., Sulatanik, E., Naik, G., Howley, I., Peysakhov, M., Cicirello, V.A., Kam, M., & Regli, W. (2005). Service-based computing on manets: Enabling dynamic intero-perability of first responders. *IEEE Intelligent Systems, 19* (5), 17-25.

Kung, S.Y., Mak, M.W., & Lin, S.H. (2005). *Biometric authentication.* Upper Saddle River, New Jersey, Prentice Hall Professional Technical Reference.

Leighton, F.T. (2004). Hearing on the state of cyber security in the United States government. *Computer Security Journal, XX* (1), 15-22.

Lindqvist, U. & Porras, P. A. (2001). eXpert-BSM: A host-based intrusion detection solution for Sun Solaris. *Proceedings of the 17th Annual Computer Security Applications Conference*, 240-251.

Maiwald, E. (2004). *Fundamentals of network security*. New York, New York, McGraw-Hill/Technology Education.

Manikopoulos, C. & Papavassiliou, S. (2002). Network intrusion and fault detection: A statistical anomaly approach. *IEEE Communications Magazine*, *40* (10), 76-82.

Mena, J. (2004). Homeland security connecting the DOTS. *Software Development, 12* (5), 34-41.

Meystel, A.M. & Albus, J.M., (2002). *Intelligent systems architecture, design, and control.* New York, New York, John Wiley & Sons, Inc.

Miller, S.K. (2001). Facing the challenge of wireless security. *IEEE Computer*, *34* (7), 16-18.

Moore, D., Paxson, V., Savage, S., Shannon, C, Stanford, S., & Weaver, N. (2003). Inside the Slammer worm. *IEEE Security & Privacy, 1* (4), 33-39.

Passino, K.M., & Ozguner, U.U. (1996). Intelligent control: From theory to application. *IEEE Expert Intelligent System and Their Applications*, *11* (2), 28-30.

Ramanujan, S. & Capretez, M.A.M (2005). ADAM: A multi-agent system for autonomous database administration and maintenance. *International Journal of Intelligent Information Technologies, 1* (3), 14-33.

Rodd, M.G. (1992). Real-time AI for industrial control: A review. *ICARV '92 Second International Conference on Automation, Robotics and Computer Vision*, Singapore, 36-38.

Russell, S. & Norvig, P. (2003). *Artificial intelligence a modern approach* (2nd ed.). Upper Saddle River, New Jersey: Prentice Hall.

Rychtyckyj, N. (2005). Intelligent systems for manufacturing at Ford Motor company. *IEEE Intelligent Systems, 19* (5), 16-19.

Tassabehji, R. (2005). Information security threats. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking (*pp. 404-410). Hershey, Pennsylvania: Idea Group.

Turban, E., Aronson, J.E. & Liang, T-P. (2005). *Decision support systems and intelligent systems* (2nd ed.). Upper Saddle, New Jersey: Prentice Hall.

Volonino, L. & Robinson. (2004). *S.R. Principles and practice of information security*. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Wallich, P. (2003). Getting the message. *IEEE Spectrum*, *40* (4), 39-42.

Wang, F-Y. (2005). Agent-based control for networked traffic management systems. *IEEE Intelligent Systems, 19* (5), 92-96.

Wang, W. (2005). The intelligent proactive information assurance and security technology. Retrieved on January 5, 2005, from http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2Fhosteddocs%2Eittoolbox%2Ecom%2FIntelligentIPDMTheWinningFormula%2Epdf

Willow, C.C. (2005). A neural network-based agent framework for mail server management. *International Journal of Intelligent Information Technologies, 1* (4), 36-52.

Yang, L. & Wang, F-Y. (2005). Driving into intelligent spaces with pervasive communications. *IEEE Intelligent Systems, 19* (5), 12-15.

Yao, Y., Wang, F-Y., Zeng, D. & Wang, J. (2005). Rule + exception strategies for security information analysis. *IEEE Intelligent Systems, 19* (5), 52-57.

Zahedi, F. (1993). *Intelligent systems for business expert systems with neural networks*. Belmont, California: Wadsworth Publishing Company.