EMJ MS
EUROPEAN MULTIDISCIPLINARY JOURNAL OF MODERN SCIENCE
https://emjms.academicjournal.io/index.php/ Volume:5

Intelligent System for Information Security Management: Architecture and Design Problems

O'rinov Nodirbek Toxirjonovich
Teacher, Department of Information Technology, Andijan State University

Abduraxmanov Jamolidin Komoldinovich
Candidate of physical and mathematical sciences, Department of Information Technology, Andijan State University

Abstract: The limitations of each security technology, combined with the rise in cyber attacks, are affecting the effectiveness of information security management and increase the amount of work that must be performed network administrators and security personnel. Therefore, there is a need to increase the automated audit and intellectual reporting mechanisms for cyber trust. Intelligent systems are emerging computing systems based on intelligent methods that support continuous monitoring and control of the plant. Intelligence improves a person's ability to make better decisions. This article presents the proposed architecture of an intelligent information security system. Management (ISISM). The purpose of this system is to improve security management processes. such as monitoring, control and decision making with an effect size that is higher than security expert, providing mechanisms to enhance active knowledge building about threats, policies, procedures and risks. We focus on the requirements and design challenges for base Components of an intelligent system.

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

Cyber Security Review

The exponential growth of the Internet, the convergence of the Internet and wireless multimedia applications and services are creating new security challenges (Miller, 2001). Security is a complex system (Volonino, 2004) and should be taken into account at all points and for each user. Organizations need a systematic approach to managing information security that consistently addresses security issues everyone level. They are need systems that support optimal distribution from limited security Resources on the based on predicted risk rather than perceived vulnerability. However, the security infrastructure... In most organizations, there was a need, not planning based on reactivity approach such as finding vulnerabilities and applying software updates (Cardoso & Freire, 2005) as opposed to a proactive approach (Gordon, Loeb & Lucyshyn, 2003). On the other side, cyber security plans call behind more specific requirements behind computer and network security also as accent on the availability commercial automated audit and re- transfer mechanisms and promotion safety assessment products and threat management (Chan and Perrig, 2003; Hwang, Tseng and Tsai, 2003; Leighton, 2004).

Except technical security controls (firewalls, passwords, intrusion detection, disaster recovery plans, etc.), justice from en organization includes other issues that are usually related to processes and people, such as policy, training, habits, awareness, procedures and many other less technical and non-technical issues (Heimerl and Voight, 2005). Security education and

awareness lags behind rapid and widespread use new digital infrastructure (Tassabehji, 2005). All these factors make security a process that based on interdisciplinary methodologies (Maiwald, 2004; Mena, 2004). Existing problems Information security management, coupled with a lack of scientific understanding of organizational behavior, requires more advanced computing systems that support the efficient use of specific information technologies and new approaches based on intellectual methods and information security as a means of coordinating and exchanging information. Intelligent systems appeared as new software systems to support complex applications. In this article, we propose an architecture for Intelligent Information Security Management System (ISISM) that maintains security processes and infrastructure within the organization. Among these components are intelligent systems include intelligent agents that demonstrate a high level of autonomy and function successfully in situations with a high level of uncertainty. The system supports knowledge acquisition, which is likely to help the human user, especially at deeper levels of understanding and problem solving for Information security guarantee domain.

The following section of this document provides a summary of information security management issues . and trends, a brief overview of information security threats followed by an overview of artificial intelligence technologies. Nikes for cybersecurity applications. We then show the architecture and main components intelligent system and include specific requirements for the design of intelligent agents. We are dis- discuss key issues related to design and technology using a systems engineering approach. We discuss that systems based on agent-based intelligent control provide a way to analyze, determine signing and implementation of complex software systems. We end with an outlook on the future of efficiency and effectiveness of information security management by applying multi-paradigm an approach.

Information Security Control

Problems and Trends

Information security management is the foundation for ensuring the effectiveness of information. security control of information resources. It is designed to monitor and control security issues related to compliance with security policies, technologies and actions based on decisions made by Human. The goal of information security management is to ensure non-repudiation, authenticity, confidentiality, integrity and availability of information within the organization. Despite the fact that Various security technologies support specific security features, and there are many issues that affect effective information security management. These technologies are inefficient and scalable because they rely on human experience to analyze data periodically. Many devices and systems generate hundreds of events and report various problems or symptoms. In addition, all of these devices may ship at different times and from different vendors with different reports and data. management options and, perhaps worst of all, different update schedules. Security technologies are not integrated and each technology provides information in its own format and meaning. These systems, running across different versions, product lines, and vendors, may provide little information. or lack of consistent characterization of events that present the same symptom. These technologies lack of functions for aggregating and analyzing the collected data. In security analytics management must choose how best to select observations, highlighting aspects of interest. A static snapshot provided by a single security technology (safeguard) does not provide the type of insight needed. behind predictive analysis.

Organizations rely on a person, such as a network administrator or security personnel, to regularly query another Database behind new vulnerabilities and apply patches to them systems to avoid attacks.

Quite often, different security personnel are responsible for monitoring and analyzing the data provided. under a single system. Reports indicate that security personnel periodically do not analyze data and fails to timely aggregate and communicate to all parties the results of analytical reports. associated with security management. In addition, the tools used have very little impact on security. prevention, because these systems lack the ability to generalize, learn, and adapt in time. Well rental security technologies lack integration, prediction, and real-time human feedback to take steps to prevent or stop the attack. In addition, technologies are inefficient for large-scale attacks. In addition, the limitations of each security technology, combined with the rise in the number of attacks affect the effectiveness of information security management and increase the number of actions that network administrators must perform. Specific issues include data collection, data reduction, normalization, event correlation, behavior classification, reporting and response. To provide a complete, accurate and comprehensive picture of network events required by network administrators, a huge amount of near-real-time event processing, consolidation and correlation from events are needed.

Therefore, comprehensive solutions are needed, including detection and filtering of attacks, source tracking and identification, and attack prevention and preemption (Chang, 2002). There is the need to expand automated audit mechanisms and intelligent reporting that support security assessment and threat management. Savely in his book "Prologue to Giarratano and Riley "said that" the key to automation and our future lies in the effective application of the field of computer science called artificial intelligence" (Giarratano and Riley, 1989). Solutions that support real temporal analysis of threat data is very important because real-time detection allows security personnel to prevent intrusion early in the attack cycle. This leads to a reduction in the harm caused by successful attacks, as well as reducing the risk of data loss and the need to perform recovery and extensive forensic examination after the incident.

IBM manifesto (Kefart & chess, 2003) points from difficulties in control calculations systems because their complexity approaches the limit of human capabilities, while there is a need for increased connectivity and integration. Systems become too complex even for the most qualified system integrators for installation, configuration, optimization and maintenance. Information security management is no exception. One of the proposed solutions is autonomous computing systems that can manage themselves according to the high-level goals of administrators. These systems require capabilities for self-tuning, self-optimization, self-healing and self-protection. Unfortunately, successful offline computing still in future, many years far.

In contrast to autonomous systems, another trend is related to systems focused on effective interaction between a person and an agent. interaction. For example, security policies can control the execution of an agent and communicate with a human to ensure that the agent's behavior conforms to the desired security constraints and goals politics (Bhatti , Bertino , Ghafur & Joshi, 2004; Bradshaw, Kabri & Montanari , 2003). Security Event management solutions are needed to integrate threat intelligence across multiple security systems and networks. products for rejecting false alarms, correlating events from multiple sources, and identifying significant events to reduce unmanaged risks and improve operational security efficiency. Exist the need for greater use of automated tools to predict the occurrence of attacks on security systems. Audit and intelligent reporting mechanisms should support security assessment and threat management on on a larger scale and in correlation with past, current and future events. Automated de- increase the burden on a person to process important data collected from different sources. Also, they significantly reduce the time of obtaining information from several systems and reduce the risk of missing possible attacks.

Effective information security management requires an approach to managing security events with advanced real-time capabilities, adaptation and generalization to predict possible attacks and support human action. Dowd and McHenry (1998) note that "network security should be it is better understood and hugged" and recommend strategies for example , knowing in potential attacker, the value of protected assets, and understanding sources of risk such as a poorly administered system, social engineering, external or internal intrusion. To provide protection against For the latest generation of cyber threats, proactive protection rules must meet criteria for efficiency, performance, and protection. The effectiveness of a security management system is determined by the intelligence of a system, defined as the ability to accurately detect unknown attacks. along with enough time strategically take action against intruders (Vanga, 2005).

Information Security Threats

Information security threats are secret in two categories (Tassabedji , 2005):

- Technical sources such as intrusions, probing or scanning, automatic listening, automated password attacks, fake, denial service attacks, and malware
- Non-technical, such as natural disasters, attacks on physical infrastructure, human error, and social engineering.

If organizations were to use an automated tool to analyze network behavior, the damage caused on slammer worm could have was strongly reduced or shunned in January 2003. the worm infected at least 75,000 hosts and caused disruption to business and daily activities (airline flight cancellations, election interference, and bank ATM failures) (Moore et al., 2003). The worm spread very quickly from one network to another. Worm caused a lot of network traffic, bandwidth consumption, network equipment and database server crashes due to resource exhaustion (CPU and memory), as well as internal DoS attacks, including increase in multicast traffic. If all these measurement trends were analyzed and the correlations were performed by a smart tool, the damage caused by this worm could be greatly reduced or avoided. Interpreting network traffic requires consideration of many things and requires to logically analyze lots from data for draw en interpretation or conclusion in a short time.

Effective information security management requires an understanding of the detection and exploitation processes used to attack. Typically, an attack is a set of steps. First phase discovery or network intelligence. The attacker gathers information about the target using public databases and documents; and more invasive scanners and grabbers. The attacker then attempts to discover vulnerabilities in the identified services, either through additional research or using a tool designed to determine the vulnerability of a service. In terms of damage scanning is usually harmless. Intrusion detection systems classify scans as low-level attacks because They not harm servers or Services and network administrators ignore This Information.

However, scanning is a precursor to attack. If a port is found open, there is no guarantee that the attacker will not return, but is more likely to return and the attack phase will begin. Some services and applications are targets for attacks. Despite the use of security technologies, the network administrators must decide how to protect systems from malicious attacks and unintentional cascading failures. One method, called reconnaissance, is used by hackers to select networks and domains to find targets. Intelligence allows a hacker to identify targets for attack or used to launch attacks. Targets are systems or networks with vulnerabilities. In order to protection from potential intruders, it is necessary to understand their methods of

reconnaissance and causes. For example, knowing the goals of hacker intelligence, network administrators and security staff can check goals and improve in security goals or in network.

Therefore, monitoring and analysis of hacker intelligence models must be carried out correctly . and continually determine the impact they can have on safety management. In the soup To move these activities, network administrators and security personnel need automated and efficient technology for recognition and analysis intelligence patterns.

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

Artificial Intelligence Techniques

Artificial intelligence methods such as data mining, artificial neural networks, fuzzy logic and expert systems can integrate with traditional procedural and statistical methods to analyze the collected data by sensors , recognize intelligence patterns, filter and correlate events to support security events control and intrusion prevention. These methods improve the ability of security management systems to correlate events generated by a diverse set of modern tools used to network management and security monitoring (Hentea , 2005a). Statistical methods have been used to build intrusion and fault detection models (Manikopoulos & Papavassiliou , 2002), but these models be unable to learn and adapt to time.

Expert systems are the most common form of AI used today in manufacturing, telecommunications, business and other areas. For example, Sun Microsystems has developed a host intrusion system. discovery system using expert system methods for the Sun Solaris platform (Lindqvist & Porras, 2001). Systems based on an expert system and inference methods are inefficient . and scalable, as they rely primarily on human experience, known facts, and statistics implemented in host or network-specific rules, and are limited in scope. However, the expert systems developed to a new trend from integration with in traditional Information treatment such that in the early nineties, expert systems merged into a new knowledge-based infrastructure. technology.

Knowledge-based systems, artificial neural networks, and fuzzy logic are the most promising AI approaches for applications such as failure and event monitoring, detection, isolation, diagnostics, supervisory and adaptive control, direct control (Rodd, 1992). Adaptive control refers to the ability of a system to regulate (adapt) itself to achieve a desired outcome despite a change in control the goals and conditions of the process or unmodeled uncertainties in the dynamics of the process. Techniques related to intelligent control include fuzzy, expert, and neural control (Hentea , 1997; Passino & Ozguner , 1996). Intelligent systems have been developed to automate production in Ford Motor Company (Rykhtitsky , 2005).

Artificial intelligence methods expand the capabilities of agents. Smart Agents and Multi-Agent systems are one of the fastest growing areas of research and development. Vulnerability agent-based intrusion detection and scoring are discussed in (Cardoso & Freire, 2005). Issues of designing and implementing a multi-agent environment for a stand-alone database administration system and security are described in (Ramanujan & Capreteuse , 2005). Strategies behind security _ Information analysis and data booty technology to discover hidden Information about possibly cyber threats are discussed in (Yao, wang, Zeng & wang, 2005).

BUT multi-agent system is an developed and implemented as some interaction agents. multi-agent systems are ideal for presenting problems that have multiple problem solving methods and multiple points of view. Intelligent agents take initiative where appropriate and interact socially, if necessary, with other artificial agents and people to solve their problem decision and help others in their work.

While AI-based techniques are emerging to support information security management, they remain focused on limited scope. Recently, AI techniques have been explored to build robust intrusion detection and prevention systems. Several techniques and application examples intrusion detection and prevention systems are discussed in (Hentea , 2005b). Intelligent network management systems support functions such as monitoring, diagnostics or management. specific network Resources are discussed in (Berenji , 1994; hentea , 1999; turban, Aronson & Liang , 2005). For example, the WatchGuard software includes an intelligent agent that supports limited firewall configuration management capabilities (http://www.watchguard.com). artificial neuron networks technology are proposed behind biometric identification Applications (Kung , Poppy and Lin, 2005). A neural network agent based system for mail server management is discussed in Willow (2005).

Artificial intelligence methods can be used to build intelligent models to improve information security. management capabilities, intrusion detection and prevention, security event management efficiency and decision making (Hentea , 2003, 2004, 2005b , 2005c). intelligent systems called intelligent assistants assist users in the decision-making process to configure and monitor specific metrics, correlate failures and events that can lead to attack reconnaissance and cyber attack prevention. Effective information security management requires intelligent a system that supports a real-time enhanced security event management approach, adaptation and generalization to predict possible attacks and support human actions. The following section describes the main components and main functions of the intelligent system for Information security management (ISISM).

IZSM Architecture

Any reasonable system composed from two parts (Meistel & Albus , 2002):

1. Internal, or computational, which can be decomposed into four internal intelligence subsystems. following:

a. Sensory processing - input to intelligent systems comes through sensors and processed to create consistent state from in World. Sensors are used to monitor in state outside world and rational system myself.

b. Modeling the world is an assessment of the state of the world; it includes knowledge bases about the world and contains a modeling module that provides information about future states of the world.

c. Behavior generation is a decision-making module that selects goals and plans, and performs tasks.

d. Value judgment - evaluates both the observed state and the predicted state; it provides in basis for making a decision.

External, or interface; entry and exit from the inside of intelligent systems are summarized through sensors and drives that it could be considered outer parts.

In all intelligent systems, the sensor processing subsystem processes data from sensors to obtain and maintain an internal model (representation) of the world. The behavior generation subsystem then determines the order of actions to be taken to achieve the goal. Behavior generation the system controls the executive mechanisms to achieve behavioral goals in the context of the perceived model of the world. Intelligent system outputs generate commands or actions to control the target system. Sensor data is the basis for creating knowledge bases, obtaining new knowledge, detecting and predicting cyber threats . attacks and make timely decisions. Examples of sensor data include measurements related to performance, security, status for the following:

Device such as processor performance, memory usage, disk space used, file usage, number of active connections, number of open connections, number of failed logins, number of transactions (requests, updates, deletes), new user requests, new software requests , user completion, response time, number of privileged users accessing the system at the same time, number concurrent users, configuration changes, file access per user, number of system calls, number of warnings, number of user authentication failures, number of pending connections, timeout periods, program execution time, system file usage, shared library usage, hours synchronization protocols, system clock, user access to data and executable files, log files the size, etc.

- Network such as available bandwidth, latency, network access requests, amount of resources unavailable for some time, new protocol requests, number of ports open at the same time, the number of simultaneous transactions over the Internet, the number of simultaneous transactions on the internal network, configuration changes, excessive noise on the channel requiring retransmission, the number of lost packets, the number of email messages, the number of console messages, protocols use, etc.
- Interfaces such as usage statistics
- Environmental (temperature, doors open, doors locked, alarms)
- Security guarantees (firewalls, intrusion detection systems, antivirus software, virtual private network, encryption) such as: number of rejected connections, number of warnings, number of false positives, number false negatives, downtime, maintenance time, number of software updates, reconnaissance activities, number of encrypted and decrypted keys, repeated mote accesses, etc.
- Security politics (problem the date, revised the date, goals, etc.)
- Risks (accepted, reduced, transferred)
- Unseen circumstances and recovery plans
- Actions of security and network administrators (logins, configuration changes, installed software, software updates, testing, number of notifications, user applications executed, etc.).

We adapt the system architecture specified in (Meystel & Abus , 2002) which is based on real control system (RCS) methods. Meistel and Albus (2002, p. 19) note that "intelligence in systems it is created by a certain architecture that organizes joint functioning otherwise smart devices. All elements of the intellect are based on an elementary functioning loop (self-management). containing an agent), which allows you to create functional relationships and information flows. figure 1 shows the main components of a standalone security agent. Enterprise cybersecurity is observed and/or controlled, or serves as an environment for an elementary cycle of operation activities.

An agent has perceptions (through sensors) as its inputs and actions as its outputs (produced by effectors called actuators). Software agents are repeating computing units. many times within an intelligent system at many different levels as units of information in all subsystems are aggregated into entities , events, situations and goals are decomposed into sub-goals and generate actions or commands. In each cycle, the safety sensors process and security modeling maintain a knowledge base with a characteristic range and resolution. At each level, plans are drawn up and updated with different planning horizons. At each level, briefly the terminal memory tracks sensory data over various historical data intervals. Feedback at every level control loops have a characteristic. For example, the controlled variables could be throughput and network latency. This model of a multi-level hierarchy of computing cycles

gives a deep understanding of the phenomena of behavior, perception, cognition, problem solving and education.

The architecture of an intelligent system is a specific frame of agents, and each agent has its own own architecture. Any intelligent system is also based on the concept of a generalized agent. Agents with similar functions can be gradually combined into a group type agent, which is a generalized agent. The group agent gives a new representation of the world (or a new granulation, or a new resolution). Further, Group agents can be aggregated in en even more generalized agent (Group groups of agents) in a hierarchical structure. This architecture supports the information security model control.

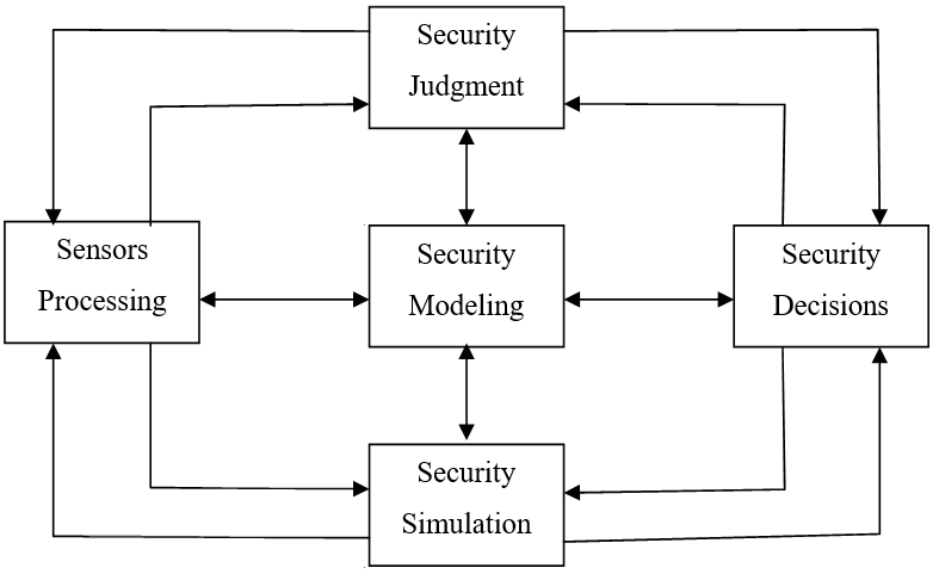

Figure one: Autonomous agent, adapted from (Meistel & Albus 2002)

Software agents that can change their location in the system are called mobile agents. Mobile agents can roam the network and perform tasks on other machines. This allows processes migrate from computer to computer and return to the starting point. In addition, process migration allows executable code to navigate and interact with databases, file systems, information services, and other agents. Mobile agents are used to discover network services on live wallets (mobile ad hoc networks) environments (Kopena et al , 2005). Intelligent spaces based on intelligent design vices are becoming commonplace applications in smart homes, workplaces, classrooms, hospitals and transport services (Yang and Wang, 2005).

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

On fig. 2 shows the proposed intelligent assistant system architecture based on the integration of traditional statistical methods and various artificial intelligence methods to support the overall system, which works automatically, adaptively and actively.

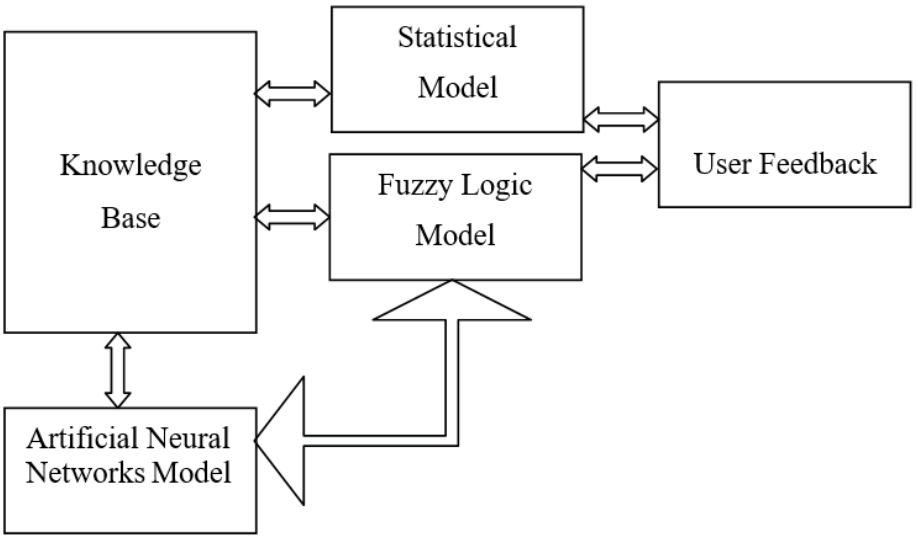

Figure 2: Reasonable Model Components

The system architecture is based on a hybrid approach providing both robustness and depth understanding decision making using intelligent models. This system aims to improve monitoring and decision-making processes with an effect size higher than that of a security expert. In addition, this system provides mechanisms for enhancing active knowledge construction. about threats, policies, procedures and risks. The model is adaptive and supports processing and classification of events and data that results in to prediction attacks. Any emergence of activity can be considered event, from Run in virus scanning software to registration in device.

One of the main design components is the development of an intelligent model for analysis and real-time event and data correlation to enhance detection and prevention capabilities security technologies: intrusion detection systems, firewalls, antivirus software, spam filters, vulnerability assessment systems, etc. For example, neural and fuzzy models should be adaptive and support the processing and classification of events and data, leading to attack prediction and advising the user through a user feedback interface. In addition, the fuzzy logic model supports the risk management, a critical stage in the information security management lifecycle (Hentea , 2006). Models should also be expanded to include information from safety plans and measures. for network monitoring, auditing, physical and logical access control. Models must support tasks for information security control such as monitoring, detection, identification from threats, as well as the prevention of attack by taking preemptive action when necessary, providing useful Information about continuous attack and prediction possible attacks.

The sounding results are encoded, filtered and processed in the sensor processing component, and subordinate to other components of the autonomous agent (elementary functional loop) shown in fig. 1. Any component of an elementary functional circuit may include one or more models from Figure 2. Data is an passed to security simulation, security modeling, or behavior genus- components that organize, classify, combine, and correlate data or generate new knowledge that stored in the knowledge base.

The hybrid system is an integration of various models of adaptive security event management, including AI methods and other methods based on statistical and traditional procedural data. an approach. The main idea behind multiple models is to perform different functions independently. with different indicators, and complement the weaknesses of one model with the advantages of another. other model. For example, artificial neural networks

can be used to classify intelligence data. patterns, but exits or options can be presented to a fuzzy logics expert system that can interpret data for humans. Since the results of the models are uncertain and imprecise in some situation, and human experts may have some intuition or knowledge about the characteristics presented information, an expert model based on fuzzy logic can improve the results of artificial neural analysis. networks model or simply interpret the results of other models in a way that is more human-friendly. In addition, the fuzzy logic model can be used to learn fuzzy rules when there is no a priori knowledge. about fuzzy regulations and fuzzy sets.

The model is based on agent technology for monitoring, detecting and identifying threats, as well as preventing an attack by providing useful information before an attack occurs. Agent Based Application plications have was used in production, process the control, telecommunications systems, air traffic management, traffic and transport management, information filtering and collection, electronic commerce, business process management, entertainment and healthcare (Jennings , Sycara & Wooldridge , 1998). Wang (2005) discusses agent-based intelligent network traffic management. control systems and transport systems.

The system should include features for automated tasks such as data collection, data processing, filtering and correlation of events based on multi-agent technologies. Intelligent agents support information security measurements, monitoring, analysis and control. The system can generate commands to end processes or transfer processing to another device if there are signs of a suspicious behavior or failures are discovered. Devi & Ramachandran (2002) describe multi-agent system behind network management, where agents negotiate the performance of processors in a cluster network when service speeches are lowered.

In addition, our system is an intelligent assistant that provides users with feedback, such as assistance in creating decisions and taking actions. In addition, the system must include a media-based user interface to support network administrator operations and a knowledge base for maintenance. reliability as systems change and adapt. This knowledge base should be adaptive and public. via web. Verification of computer generated solutions can be done by comparing with expert decisions. In addition to automated knowledge search methods, this method allows you to build a knowledge base for making decisions and actions using human experience and judgment.

The user feedback module should provide various feedback to the network administrator or security personnel. 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, without specific information about individual changes or predictions, but whether the training program can suggest new strategies and changes. This is an important aspect of machine learning. Much of the research in machine learning has focused on learning rather than creation. feedback as useful information for the user to make a decision. Purpose of an intelligent system is an on the development of teaching methods that can support business and advice the user to make decisions before an attack corrupts information or renders systems inaccessible. Another important factor to consider is that security systems and policies change on their own. over time and across platforms and enterprises. These special circumstances must easily and timely be included in the machine learning program to support the user. In addition the car education program should support a knowledge base to enrich in education Environment.

Design Problems

The main decision to be made during architectural design is which agents should be included. Several types of agents can be developed to support information security management (Russell & Norvig , 2003). In the proposed system, key agents should be decision makers and responsible persons. troller agent.

An intelligent agent is seen as a combination of functionality and intelligence. (ability to act in an uncertain environment, learning ability, adaptability, probability of success). Functionality (called roles in some methodologies) is what agents will perform by looking at with combinations of functionality. While there has been much debate about what constitutes agent, and what features are important, the consensus is that a reasonable agent is located, autonomous, reactive, proactive and social. The main contribution to the field of autonomous agents it is artificial intelligence.

Due to in complexity from Information security control tasks, in proposed system based on on the integration of various types of intelligent agents, real-time hybrid architecture restrictions. Intelligent agents help automate various tasks such as collecting information, filtering and using it for decision support and can help improve network performance. administrator. The design and programming of agents should focus on maximizing their performance metrics, which embody the agent's behavioral success criteria (Russell & Norvig , 2003). Other important issues to be addressed include the portability, stability, resiliency, and security of agents and systems (Bradshaw et al, 2001; Hamidi & Mohammadi, 2006). The interface should demonstrate intelligent features that help the user make decisions and take actions. control the security process.

Performance indicators should be developed according to what is needed in the environment information security management, and not in accordance with how, in the opinion of the agent, should behave. In addition, at the design stage, it is necessary to determine the type of feedback available for learning . because it is usually the most important factor in determining the nature of a learning problem. faced by the agent. In the field of machine learning, a distinction is usually made between supervised and unsupervised learning. The scope of information security management is broad and requires the use of one or a combination of both forms for best results. Another characteristic that consideration should be given to mobility, which is the extent to which agents travel across network.

In addition, data representation (inputs to training models and outputs models) plays an important role in design. Another factor in the design will be considered having prior knowledge of some information security management tasks. Majority learning will start without any knowledge of what the agent is trying to learn. Education occurs as the agent observes its interaction with the environment and its own decisions. manufacturing processes. Learning is a process of self-improvement and therefore an important trait reasonable behavior.

The functions performed by each component can be developed along a development spiral. method. The ISISM feature set is based on the security requirements of each organization. The order in which models are implemented depends on resources and needs . next is an a brief description from Peculiarities as they were developed and used in another projects:

- Data mining supports the automated analysis and interpretation of data and events collected from different sources, as well as the discovery of relationships between data and events . and feedback from the human user. Examples of using methods and knowledge of data mining opening are discussed in (hentea , 2004; Ibrahim Folorunso and Adjayi , 2005)

- Artificial neural networks support the classification, association, and prediction of future cyberattacks by learning and adapting to past and current data and events. For example, intelligence models can be classified using neural networks based on unsupervised education (Hentea , 2005b, 2005c)
- Fuzzy logic allows you to process qualitative variables and draw approximate conclusions when suggestions are inaccurate and vague. One model is used for risk assessment (Hentea , 2006)
- Reasonable help and user Feedback technology are discussed in (Hentea , 1997)
- Statistical approaches who discussed in (Hentea , 1997 2006).

However, the synergy between different approaches can help improve and highlight the qualitative aspects of each model, thus creating knowledge and intelligence that helps the individual. make decisions. Possible path for integrating data mining, neural networks and fuzzy expert systems in the fight against intrusion attempts will use data mining and a neural network detect and classify patterns of intelligence and its attributes. This information may be passed to a fuzzy expert system, which can then advise the person to take action based on the status of intrusion attempts. In addition, neural networks can recognize patterns and predict possible cyber attacks. Also, neural networks can draw conclusions from fuzzy or inaccurate data about a particular situation. Knowledge base includes security knowledge areas such as raw data and events, performance metrics, patterns, policies, and decisions. AT In addition, knowledge refinement, knowledge representation and knowledge discovery are important components of a knowledge management system. Another requirement is the cost of development and maintenance. The system must be cost-effective so that organizations can afford to use advanced technologies (data mining, artificial neural networks, fuzzy logic and knowledge base) to protect and prevent security breaches (Wallich , 2003). Although we have described several possibilities for the system, we have not provided an exhaustive list of requirements. in- The purpose of this article is to provide a framework for developing an intelligent system for information processing. security management. Similar intelligent systems for manufacturing are described in (ISAM, 2007).

Conclusion

Advanced real-time workflows based on simulation, sensory 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 methods support the ability to provide automated feedback for troubleshooting, including helpful human tips actions and prevent ongoing attacks. We propose a new intelligent system architecture for information security management. The proposed architecture is based on an interdisciplinary paradigm that includes information security management, network communications, and automata. (process management), computer science, artificial intelligence, modern management theory, statistics, social sciences, organizational theory and behavior, management science, business strategies, risk analysis and economics. No single approach can solve the problem of growth and complexity cyber threats (Gordon , Loeb & Lucyshyn , 2006). We need to apply several paradigms to satisfy Information Security Management Challenges for the Modern Organization of the $^{21st\ Century}$. century. Based on groundbreaking work in artificial intelligence and other fields, intelligent agent technology is widely used in cybersecurity. Intelligent agent technology is being considered by some scholars. search engines should become the natural successor to object-oriented programming. No prototypes or systems this species has been identified. However, individual function or component prototypes appear, but these components require deeper development and integration. The

system should be adaptive and able to discover and create new knowledge for information security domain. Future work should aim for a systematic proof of concept that integrates all modules to support security management.

Recommendations

1. Berengi, HR (1994). unique strength from fuzzy logics the control. *IEEE Expert*, *nine* (4), 4.
2. Bhatti, R., Bertino, E., Gafur, A., & Joshi, JBD (2004). XML-based specification for web services document security. *IEEE computer*, *37* (4), 41-49.
3. Bradshaw, J.M., Suri, N., Kanas, A.J., Davis, R., Ford, K., Hoffman, R., Jeffers, R., and Reichherzer, T. (2001). Terraforming Cyberspace. *A computer, 34* (7) 48-56.
4. Bradshaw, J. M. Kabri, J., & Montanari, R. (2003). The return of cyberspace. *IEEE Computer*, *36* (7), 89- 92.
5. Cardoso, R.K. and Freire, M.M. (2005). Security vulnerabilities and risks in Internet systems and services vices. In M. Pagani, (Ed.), *Encyclopedia of Multimedia Technologies and Networks* (pp. 910-916). Her- hey, Pennsylvania, IDEA GROUP REFERENCE.
6. Chan, H. & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer*, *36* (10), 103-105. chang, PAC (2002). Protection against flood-based distributed denial of service attacks: BUT management. *IEEE Communications magazine*, *40* (ten), 42-51.
7. Devi, SES & Ramachandran, V. (2002). Agent-based control of embedded applications. Received de-September sixteen, 2006 from http://www.hipc.org/hipc2002/2002Posters/AgentControl.pdf
8. Dowd, PW & McHenry, JT (1998). Network security: This time to take This is jokes aside. *IEEE computer*, *31* (nine), 24-28.
9. Giarratano, J. & riley, GRAM. (1989). *Expert systems principles and programming*. Boston, Massachusetts, PWS-KENT Publishing Co.
10. Gordon, L.A., Loeb, M.P. and Lyutsishin, V. (2003). Information security spending and real options: A wait and see an approach. *A computer security log*, *XIX* (2) 1-7.
11. Gordon, L.A., Loeb, M.P. and Lyutsishin, V. (2006). Computer and Cyber Security Violations: Schumpeter in save. *A computer security log*, *XXII* (4), 9-10.
12. Hamidi, H., & Mohammadi, K. (2006). Modeling the fault-tolerant and secure execution of mobile agents at a distance tribute systems. *International Magazine from Reasonable Information Technology*, *2* (one), 21-36.
13. Hamerl, J. L. & Voight, H. (2005). Measurement: the basis for developing and managing a security program. ment. *Journal of Computer Security*, *XXI* (2), 1-20.
14. Hentea, M. (1997). Architecture and design issues in a knowledge-based hybrid expert system for intellectual - gentleman qualitative the control. PhD Thesis, Illinois Institute from Technology, Chicago, Illinois.
15. hentea, M. (1999). Reasonable an approach behind network control system: Architecture and design questions behind ATM a computer networks. *Proceedings from 1999 Advanced Modeling Technology conference*, San Diego, California.
16. Hentea, M. (2003). An intelligent model for detecting and preventing cyberattacks. *Proceedings of ISCA 12th international conference Intelligent and Adaptive Systems and Software Engineering*, San Francisco. sisco, California, 5-10.

17. Hentea, M. (2004). A descriptive data mining model for intrusion detection systems. *materials 2004 International Conference of the Information Resource Management Association,* New Orleans, Lu- Isiana , 1118-1119.
18. Hentea, M. (2005a). Information security management. In M. Pagani, (ed.), *Multimedia Encyclopedia. technology and network (*p. 390-395). Hershey, Pennsylvania, IDEA GROUP REFERENCE.
19. Hentea, M. (2005b). Increasing Intrusion Awareness with a Neural Network Classifier. *materials ISCA 14th International Conference Intelligent and Adaptive Systems and Software Development*, To ronto, Canada, 163-168.
20. Hentea, M. (2005c). Using intelligence templates for a smart monitoring model. *materials 2005 Information Resource Management Association International Conference*, San Diego, CA-nya 160-163.
21. Hentea, M. (2006). Improving information security risk management with a fuzzy model. *Proceedings 19th International Conference on Computer Applications in Industry and Engineering*, Las Vegas, Nevada, 132-139.
22. Hwang, M3-S. Tseng, SF. and Tsai, CS. (2003). New Secure Generalization of Threshold Signature scheme. *Proceedings from International Technology behind Research and education*, 282-285.
23. Ibrahim, S.A., Folorunso, O. and Adjayi, O.B. (2005). Discovery of knowledge about closed patterns of frequent calls terns in the telecommunications database. *Proceedings of the conference "Information Science and IT Education" for 2005 Joint Conference,* Flagstaff, Arizona, 137–148. Can be bought at http://proceedings.informingscience.org/InSITE2005/P13f80Ibra.pdf
24. ISAM. (2007). Intelligent Systems Architecture for Manufacturing (ISAM): Reference Model Architect - for Intelligent Manufacturing Systems. Retrieved January 15, 2007 from http://www.isd.mel.nist.gov/projects/rcs/isam/ISAM_web.htm#framework
25. Jennings, N.R., Sicara, K. & Wooldridge, M. (1998). Agent research and development roadmap. Hotel. Jennings, C. Sicara, M. Georgeff (eds.), *Autonomous Agents and Multi-Agent Systems, 1* (1), pp. 7-38. Boston, Massachusetts, Klyuver Academician Publishers.
26. Kephart, J. O. and Chess, D. M. (2003). Vision of automatic calculations. *IEEE Compute*, *36* (1), 41-50.
27. Copen, J., Sulatanik, E., Naik, GRAM., hawley, I., Peisakhov, M., Chichirello, V.A., Kam, M., & Regli, AT. (2005). Service calculations on the manets: Inclusion dynamic interoperability from first defendants. *IEEE Reasonable systems, nineteen* (5), 17-25.
28. Kung, S.Yu., Mack, M.V. and Lin, S.H. (2005). *Biometric authentication.* Upper Saddle River, New Jersey Prentice Hall Professional Technical reference.
29. Layton, F. T. (2004). Hearing on the State of Cybersecurity in the US Government. *A computer Security Magazine, XX* (one), 15-22.
30. Lindqvist, W. & Porras, P.A. (2001). eXpert - BSM: Intrusion Detection Host Solution for Sun So laris. *Proceedings from in 17th ‑ Annual A computer Security Application Conference*, 240-251.
31. Maywald, E. (2004). *Fundamentals of Network Security*. New York, New York, McGraw-Hill / Technology Education.

32. Manicopoulos, K. & Papavassiliou, S. (2002). Network Intrusion and Fault Detection: A Statistical Anomaly an approach. *IEEE Communications magazine, 40* (ten), 76-82.

33. Mena, J. (2004). Homeland security linking DOTS. *Software Engineering, 12* (5), 34-41.

34. Meistel, AM & Albus, DM, (2002). *Reasonable systems architecture, design, and the control.* New york, New york, John Wylie & sons, Inc.

35. Miller SC (2001). Facing in call from wireless security. *IEEE computer, 34* (7) 16-18.

36. Moore, D., Paxson, V., Savage, S., Shannon, K., Stanford, S., & Weaver, N. (2003). Inside the prison worm. *IEEE Security & Confidentiality, one* (4), 33-39.

37. Passino, K.M., and Ozguner, W.W. (1996). Intellectual control: from theory to application. *IEEE Expert Intelligant System and Their applications _ eleven* (2) 28-30.

38. Ramanujan, S. & Capretez, MAM (2005). ADAM: multi-agent system for autonomous database. care and maintenance. *International Journal of Intelligent Information Technology, 1* (3), 14-33.

39. Rodd, M.G. (1992). Real-time AI for industrial control: an overview. *ICARV '92 Second International Conlink on the Automation, Robotics and computer vision*, Singapore, 36-38.

40. Russell, S. & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd ed .). River Upper Saddle, New Jersey: Prentice Hall.

41. Rykhtitsky, N. (2005). Intelligent systems for production at Ford Motor Company. *Intelligent IEEE systems, nineteen* (5), 16-19.

42. Tassabeji, R. (2005). Threats to information security. In M. Pagani, (ed.), *Encyclopedia of Multimedia Technology and networks (* p. 404-410). Hershey, Pennsylvania: Idea Group.

43. Turban, E., Aronson, JE & liang, TP. (2005). *Decision support systems and reasonable systems* (2nd ed.). Upper Saddle, New Jersey: Prentice Hall.

44. Volonino, L. & Robinson. (2004). *SR Principles and exercise from Information safety*. Upper Saddle River, New Jersey: Pearson Prentice Hall.

45. Wallich, P. (2003). Receiving in message. *IEEE spectrum, 40* (4), 39-42.

46. Wang, F.Ya. (2005). Agent control for network traffic management systems. *IEEE Intelligent System tems, nineteen* (5), 92-96.

47. Wang, W. (2005). Intelligent proactive technology to ensure and secure information. Received January 5, 2005, p.

    http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2F hosteddocs% 2Eittoolbox%2Ecom%2FIntelligentIPDMTheWinningFormula%2Epdf

48. Willow, C. C. (2005). An agent environment based on a neural network for managing a mail server. *International Magazine from Intelligent information technologies, 1* (4), 36-52.

49. Jan, L. & wang, F.G. (2005). Driving in reasonable space with all-pervading communications. *IEEE Intelligent System, 19* (5), 12-15.

50. Yao, Y., Wang, F. Y., Zeng, D. & Wang, J. (2005). Rule + Exception Strategies for Security Information analysis. *IEEE Reasonable systems, nineteen* (5), 52-57.

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