Artificial Intelligence Techniques for Information Security Risk Assessment

R.Gnanabharathy

Lecturer (Sr. Gr), Department of Computer Engineering, Ayya nadar janaki ammal polytechnic college

Abstract- **The phenomenon of online social networking has evolved to include more than the teenage stereotype looking to expand his/her network of online friends. People of all ages and backgrounds have discovered that they can enrich their lives through the contacts they make on a social networking website. The social networks must progress to make the user's life easier with the aim of providing security and privacy in their day to day routine. The integration of AI techniques to solve current problems is a help to achieve intelligent environments offering adaptive behaviors depending on the user's intentions. Artificial Intelligence (AI) is one of the computer science areas with more expectation created in the last years. AI is a scientific discipline which tries to operationallies human intellectual and cognitive capabilities in order to make them available through information processing systems. Nowadays, many security and privacy problems cannot be optimally solved due to their complexity. In these situations, artificial intelligence has proven to be extremely useful and well-fitted to solve these problems. Artificial neural networks, evolutionary computation, clustering, fuzzy sets, multi-agent systems, data mining and pattern recognition are just a few examples of artificial intelligence techniques that can be successfully used to solve some relevant privacy and security problems.**

Index Terms- SMTP, NLP, GA, IDS, RBS.

I. INTRODUCTION

Social networking is described as software that lets people interact, connect, play or collaborate by use of a computer network. This definition covers the popular social networking sites, including blogs, wikis, podcasts, tags, and more recently, search engines. Even more recently, the use of online communities to establish and build connections among those with shared interests has become part of the corporate world as well. As professional social networks such as LinkedIn and Blue Chip Expert continue to grow, and professional groups gain in popularity on once-personal sites like Face book and MySpace, enterprise security and risk management professionals must face the reality that these sites are emerging as a source for the unauthorized disclosure of confidential corporate information. While there are numerous benefits to social network solutions, one should focus on the risks of social networks. As with all emerging technologies, social networking is advancing rapidly and security professionals need to remain aware of the risks associated with it.

There is a generation entering the workforce that assumes this technology will not only be available for their use, but is also essential to the way they communicate with colleagues and business partners. While there are many benefits that come with using social networks both internally and externally, the policy and architecture to defend against the risks must be addressed proactively and should not be taken lightly.

Security success is all about the right combination of people, process, policy and technology. This can be combated by having a network management systems which should have the abilities of intellectual reasoning, dynamic real time decision making, and experience based self-adaptation and improvement. The design of such efficient, dynamic and automated social network management framework requires support from the field of artificial intelligence. Dealing with uncertainty and inconsistency has been a part of AI from its origins. More recently, AI systems are beginning to emerge that can independently formulate, refine from observed data to uncover fundamental properties. Technologies for managing uncertainty and inconsistency have already been used in areas such as the ranking algorithms used in web search engines.

The expectation is that AI technologies can play a similarly important role in the context of security assessments. The field of Artificial Intelligence (AI) involves the design and implementation of systems that exhibit capabilities of the human mind, such as reasoning, knowledge, perception, planning, learning, and communication. AI encompasses a number of sub-disciplines including machine learning, constraint satisfaction, search and multi-agent systems, reasoning, and natural language engineering and processing.

II. ROLE OF AI TECHNIQUES

The techniques based on the principles of artificial intelligence like Neural Network, Genetic algorithm, Expert Systems and Fuzzy Inference, provide sophisticated abilities of intelligent decision making, experience based improvement and creative problem solving. For example, fuzzy logic is a superset of conventional logic that has been extended to handle the uncertainty in data. Fuzzy logic is useful in situations where it is difficult to make a precise statement about system behavior and has been applied successfully to the area of risk management. In these applications, qualitative risk descriptors, such as High, Medium, and Low, can be assigned to a range of values and calibrated as continuous quantitative input. Also fuzzy logic can be used to assess the relative risk associated with computer network assets by ranking vulnerabilities with regard to the potential risk exposures of assets and networks. Similarly fuzzy logic can provide risk analysts more information than qualitative approaches for ranking risks, to help them more effectively manage operational risks.

While the use of AI has met with both successes and defeats, its application in aspects of security metrics might prove beneficial, particularly as a means for reducing subjectivity and human involvement in performing security assessments. The newest artificial intelligence technique like Natural-language processors (NLP) closely resembles the way our brains learn. Apart from common word processor operations that treat text like a mere sequence of symbols, NLP considers the hierarchical structure of language: several words make a phrase, several phrases make a sentence and, ultimately, sentences convey ideas. By analyzing language for its meaning, NLP systems have long filled useful roles, such as correcting grammar, converting speech to text and automatically translating between languages. Similarly, natural-language processors, which actually are an array of complex algorithms, can be used to detect spam.

They can scan e-mail messages to discover the content of the messages. The algorithms can be packaged into mail-filtering software, which generally sits outside a firewall or at an application service provider's network. Artificial intelligence mail-filtering software accepts all in-bound e-mail traffic, routing legitimate traffic to a corporate SMTP server and flagging other messages as spam. Suspect e-mail is sent to a quarantine area where an administrator can view the contents to determine whether to discard it or pass it along.

Similarly AI techniques can also help to identify intrusive behavior. It uses both anomaly detection and misuse detection techniques and is both a network-based and host-based system. In recent years, Intrusion Detection System (IDS) has become one of the hottest research areas in Computer Security. Issues relevant to intrusion detection include data collection, data reduction, behavior classification, reporting and response. There is huge amount of collected data like audit data or network traffic data. Focusing on data reduction and classification, it is found that Artificial Intelligence techniques can be used in intrusion detection system. Different AI techniques, such as finite state machine, decision tree, and GA, can be used to generate rules for IDS. Out of all these techniques, applying genetic algorithm to intrusion detection seems to be a promising area. Genetic algorithm is a family of computational models based on principles of evolution and natural selection. These algorithms convert the problem in a specific domain into a model by using a chromosome-like data structure and evolve the chromosomes using selection, recombination, and mutation operators. In Genetic algorithm, one network connection and its related behavior can be translated to represent a rule to judge whether or not a real-time connection is considered an intrusion. These rules can be modeled as chromosomes inside the population.

The population evolves until the evaluation criteria are met. The generated rule set can be used as knowledge inside the IDS for judging whether the network connection and related behaviors are potential intrusions. IDS can also be implemented using autonomous agents (security sensors) and applied AI techniques to evolve genetic algorithms where agents can be modeled as chromosomes and an internal evaluator is used inside every agent. In the approaches described above, the IDS can be viewed as a rule-based system (RBS) and GA can be viewed as a tool to help to generate knowledge for the RBS.

There are so many AI techniques that can be used for solving intrusion detection tasks. In another example, Expert system can be used to solve the problem by using the computer model of expert human reasoning and it requires continuous maintenance and upgrading for performing well. Behavior classification of intrusion detection systems can be done using expert systems techniques by encoding the security policy and known attacks as well as system vulnerabilities as a fixed set of rules. User behavior that matches those rules indicates that an attack is under way.

Unlike expert systems, Rule based intrusion derives rules that explain the set of instances describing the problems and steps of solutions. In an IDS, rule based systems create and manage rules corresponding to anomalous behavior whereas classifier systems classify different types of patterns from a set of patterns. A classifier like Decision Tree tries to separate the data into two or more groups. Then it tries to separate these groups into further groups and so on until small groups of examples are left.

Artificial Intelligence technique like artificial neural network can be used for classification purpose in an intrusion detection system. Artificial neural network is a kind of information processing technique that is inspired by the biological nervous system, such as a brain, to process information. It tries to represent the physical brain and thinking process by means of an electronic circuit or software. Neural networks learn by training. Two types of learning methods are used to train a neural network: supervised where the net is trained only by both the input and output pattern; and unsupervised, where the net is trained only by the input pattern.

A neural network has one input layer, one output layer, and zero or more number of hidden layers. All these layers contain a number of neurons which are connected with each other in two ways: feedback and feed forward. Each neuron in neural network acts as an independent processing element. In intrusion detection, most successful applications of neural network are classification and pattern recognition which takes network traffic data to analyze and classify the behaviors of the authorized users and recognize the likely attacks.

Within AI, another problem solving techniques that has gained some relevance are: planning and scheduling. AI Planning systems select an order set of activities in order to achieve one or more goals and satisfy a set of domain constraints. AI Plan Recognition techniques can be used for implementing security and adaptive innovative features for social networks. A user's behavior can be detected through his actions along the social network, which causes multiple system reactions depending on the goal predicted for that user Hence AI techniques facilitate user in the creation and infusion of autonomous services within social networks with the aim of supporting and helping users in the context of security and privacy issues. The newly developed techniques can further improve security aspects related to identity theft and extortion detection and several other problems related with security and privacy issues of Social networking.

III. CONCLUSION

Social networks are excellent platforms to apply AI techniques. As social networks are growing bigger and more and more people use them to share more information, finding what people refer to read inside of them will became soon not trivial at all. AI techniques could be really helpful in organizing such information and bringing the most relevant pieces to users in a completely personalized way. The Artificial Intelligence techniques can help to outline basic categories of privacy concerns, including solutions to them. The implementation of Artificial Intelligence techniques in Intelligent Intrusion Detection System are gaining the most interest nowadays regarding its ability to learn and evolve, which makes them more accurate and efficient in facing the enormous number of unpredictable attacks. Two major techniques for machine learning are highlighted, as the use of Genetic Algorithm and Artificial Neural Network providing intrusion system with extra intelligence. Better understanding of these techniques will allow to better design different systems with features similar to Social Networks, such as Learning Management System, Digital libraries, Promotion or consumer’s feedback systems for business.

REFERENCES

[1] Bezroukov, Nikolai. 19 July 2003. “Intrusion Detection (general issues).”Softpanorama: Open Source Software

[2] Educational Society. Nikolai Bezroukov. URL: http://www.softpanorama.org/Security/intrusion_detection.shtml (30 Oct. 2003).

[3] Bridges, Susan, and Rayford B. Vaughn. 2000. “Intrusion Detection Via Fuzzy Data Mining.” In Proceedings of

[4] 12th Annual Canadian Information Technology Security Symposium, pp. 109-122. Ottawa, Canada.

[5] Crosbie, Mark, and Gene Spafford. 1995. “Applying Genetic Programming to Intrusion Detection.” In Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8. Cambridge, Massachusetts. URL: http://citeseer.nj.nec.com/crosbie95applying.html (30 Oct. 2003).

[6] Graham, Robert. Mar. 21, 2000. “FAQ: Network Intrusion Detection Systems.” RobertGraham.com Homepage.

[7] Robert Graham. URL: http://www.robertgraham.com/pubs/network-intrusiondetection.html (30 Oct. 2003).

[8] Jones, Anita. K. and Robert. S. Sielken. 2000. “Computer System Intrusion Detection: A Survey.” Technical Report. Department of Computer Science, University of Virginia, Charlottesville, Virginia.

[9] Li, Wei. 2002. “The integration of security sensors into the Intelligent Intrusion Detection System (IIDS) in a cluster environment.” Master’s Project Report. Department of Computer Science, Mississippi State University.

[10] McHugh, John, 2001. “Intrusion and Intrusion Detection.” Technical Report. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

[11] Miller, Brad. L. and Michael J. Shaw. 1996. “Genetic Algorithms with Dynamic Niche Sharing for Multimodal Function Optimization.” In Proceedings of IEEE International Conf. on Evolutionary Computation, pp. 786-791.Nagoya University, Japan.