IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5044

A System for Computing Human Deception

Najib Saylani
Hofstra University, Zarb School of Business, Department of Business Computer Information Systems and, Quantitative Methods, Weller Hall, Room 211A , Frank G. Zarb School of Business, 134 Hofstra University, Hempstead, New York 11549-1340, Departmental Phone Number: (516) 463-5716, Fax: (516) 463-4834, Email: najib.saylani@hofstra.edu

ABSTRACT

The book titled 'The Art of Deception: Controlling the Human Element of Security' by the now famous former hacker by the name of Kevin D. Mitnick and his coauthor William L.Simon presents a detailed study of how, despite all network security programs from firewalls to strong encryption, IT infrastructure are vulnerable to social engineering attacks that easily circumvent all walls and all type of encryption. Either an insider or some one external to the organization would pose as or impersonate a legitimate user of the system and have easy access to the authorized areas in the system. This process may take longer before intrusion and successive intrusions may take longer to be noticed. It is well known and widely practiced approach by organizations to log and record all users' transactions for the purpose of network auditing but it is always late to prevent damages to the IT infrastructure. While it is impossible to fully prevent all these type of schemes, it may be possible to indirectly supervise and profile accesses to the system that may be authorized but illegal. We propose a research in this important area that will target as its goal building a system by which detection of illegitimate attempt at accessing a system or detection of authorized but illegal use of the system can be explored in an automated way.

INTRODUCTION

The research's initial phases was carried in school during this summer and consisted of:

- Collecting all relevant data to the research from related scientific domain.
- Extracting the necessary and needed facts and rules from Mitnick's book (this book is more descriptive in nature but it is used as a source of good survey of some example of human deceptions).
- Conducting theoretical studies of different scenarios pertinent to the ideas outlined in the introduction (i.e. simulation of documented stories of deceptive behavior).
- Building the right supportive environment in school. The environment consists of simulating situations where deception was occurring. It is either within the network as a set of internal and external emails' exchanges, telephone conversations or person to person contact within the organization.

Given Facts

- Again, keeping attacker off your domain requires more than just adopting and implementing the best firewall and encryption system.
- The human element is the weakest link just by the fact that regardless of how robust the security built on technology is. Employee, at the least, may comprise security by not following the right protocols.
- Internal weaknesses caused by employees can open hidden doors to the outside. Problems that can go unnoticed because of the trust taken for granted in the system.
- Given all the technological innovations in securing a domain, a single person's carelessness or criminal deceptive acts can bypass all the walls of security. These technological ways, such as biometric face recognition will not work as they cannot be enforced in all internal transactions. And, in many cases most of the advanced approaches for security are too expensive to extend to every sub entity of the organization. Just think of the situation where one entity that is part of the Extranet environment not being able to afford the best security or not implementing the best protocols.

The real world's cases prove that total and infallible security does not exist and may not be possible. The reason for this is the human factor. Preventing problem from happening is attractive but not always possible. In most cases finding out that acts of deception are ongoing, stopping them to minimize their impact can very crucial.

Proposal

Figure 1 shows a typical employee environment in the IT domain.

The employee is our main object of concern in this research. Any employee, regardless of his/her responsibilities can be a source of problem. This goes from the security officer at the door, the driver of the truck to the database administrator and to the top management. The employee does not have to interact directly with the computer system. But, in this paper we will focus on a candidate set of employees similar to the one depicted in figure 1. Employee X user of the super domain (the organization) interacts with the following sub domains:

- The Intranet: with other local employees and local servers.
- The Extranet: with other employees of other super domains and their servers.
- The Internet: public domain interaction with everyone out there.
- The real world: socializing locally with fellow employees, employees of other super domain and friends and relatives.

Access to and interactions with these sub domains part of local and remote super domains is supported through primitive ways (in person meeting and socializing) or technology based (telephone, cellular, wireless, workstation…etc.) [8]

Our approach, for detecting deceptive acts in a sea of legitimate enterprise's transactions touch on all aspects of computer security and forensics and their non-computer counterparts (human-to-human interactions). Our research goes beyond unwanted computer intrusions and their consequences on the organization. Computer forensics usually is successful after the facts. Intruders may have left tracks as evidence in their digital format. These tracks are static in nature and if left untouched they will be waiting to be found and analyzed. Good tools and methodologies exist in both the research domain and the applications' domain that can be used to mine an environment for past or ongoing acts of illegal intrusions and activities.[2][6][21]

In computer forensic, incidents can be classified from minor to severe and can be categorized to relate to user application or system. We are not going to do an exhaustive overview of this field as they are very interesting and detailed articles and books about the subject [24]. For us the focus is on the human side and their actions that may or may not be reflected on the machine. We believe that there are no minor incidents and that all must be taken seriously. Nothing should be overlooked no matter what class and category it belongs to and regardless of its degree of severity.

Our proposed methodology will not be intrusive and the system should work 24/7 in real time in the background. We know what the question is "who is in charge" and the answer is human. And we are back to square one and that is the paradox. This is very similar to the paradox in network security related to storage of passwords: An important concern then will be the question of the need for an individual and independent department for overseeing this system or only top management can interact with it. Our proposed system will take advantage of techniques borrowed from the field of Artificial Neural Network and Fuzzy Logic, Natural Language processing and others. The environment that the system will be working under will be mapped onto a domain with characteristics similar to those of what is called the semantic net. In the next section, we will be presenting our approach to building such system. We can for now label this system as an expert system for detecting acts of deceptions [2][3][5][11][12][14].

This system would access all activities within the domain, look for relationship between these activities in space and time and try to check if detected patterns match stored profiles known to be historic patterns of deception [13].

In some cases, there is no need for complexity as couple of activities will raise the red flag. Think of the example of an employee known to be on vacation and at the same time while specific transactions authorized by his are going on. For the system to detect this, a knowledge base must be updated all the time with facts associated with:

- Employee status (working, ex-employee, on vacation)
- Employee location (office, field, home)
- Employee tasks (payroll, administrative, networking, safety, driver …. Etc.)
- Authorized tasks
- Restriction if any

Those were static information. Also, there is what we will label as time-dynamic statuses or activities that are associated with the employee's specific profile

A profile (employee) = function of (static profile, time-dynamic profile)

REQUIREMENTS FOR THE PROPOSED SYSTEM

For the system to exist and work a knowledge based made up of fact about objects, (people and machine), actions, events must be created. An inference engine with access to the knowledge base and whose inputs are activities associated with profiles about objects.

Before we progress further, our problem domain is detecting acts of deception affecting the organization and our knowledge domain is a complex one consisting of expertise in both computer and non computer forensic. Expertise that should enable both a human expert and our system to find correlations between employees and non-employees activities that when put together it would be inferred that deceptive transactions are occurring.[1]

We found out from our preliminary studies that our potential system should be more that just a rule based system and this will be proven shortly when listing the other requirements. For now rules for some situation are much simpler to implement.

IF visitor is a former employee AND
IF visitor is visiting His/Her former office
Then record event And review former associated privileges
IF all or some privileges were not cancelled (deleted) initiate a report And record in knowledge base.

Check if former employee is authorized to access the premises [if recorded]. If not authorized then check with safety personnel for a feedback on why he/she was allowed in and record all. Check for any activities within the computer system associated with attempted, failed and successful access to physical area or system (if access cards are needed then easy to trace as the process is already automated otherwise if other employees are to authorize access, event must be recorded and protocols must be reviewed).

And as we can observe, this simple example show the complexity of the tasks ahead and the need for a mechanism of triggering an event (former employee came to visit), adding the event to the knowledge base (security personal would record on a local database the fact that the former employee was let it) make change to an already stored event and update of existing event (case of a person mistaken for a former employee) … etc.

Note that security and safety protocols do exist in most if not all organizations but enforcing the rules is the problem. Again the human factor is the weakest link (think of a security guard allowing a former employee and buddy to enter the premises despite a specific protocol prohibiting that). A deceptive reason may be that he/she asked to get in to recover some old belonging from the locker or the office. So, as long as the visit is logged, even if the access is not authorized that should raise an immediate flag automatically by the system. In case the security guard fail to report on the visit, other redundant measures across the system should be implemented so that knowledge, even partial, can be added to the main knowledge base. Now we are at the level of discussing partial knowledge that when used by the inference engine may not trigger an early alert because of insufficient correlation between successive or non successive events related to the same object (in our example, the former employee may have entered the premises more than once in the last year, socialized with other employees, accessed the internet, printed documents, … etc.), but only months later was the main problem detected (i.e. stolen or corrupted data or even disappearance of physical item). Forensic processes may succeed in finding links between the problem and the former employee (if he/she is the culprit) but, and again because of the nature of the information available the task may not lead to good result. This can be true for our suggested system too. But, and especially when the rules of the inference engine are not enough (or intelligent enough) to come with a conclusion we need the help of methodologies other than rules based one.

FEATURES AND CHARACTERISTIC OF THE PROPOSED SYSTEM:

See figure 2 for an overall view of the entities that are part or/and associated with the system.

Our main component of the system beside the rule based one is an Artificial Neural Network (ANN). For an ANN we need historical knowledge and about deceptive act in different situation. Our system may not encounter exactly a stored pattern but should be able to converge to it. It will be easy to match a newly retrieved pattern to a historical one if they are the same. But, the convergence may trigger an alert even though no act of deception occurred. Just think of what prosecutors and law enforcement label as consequential evidences. But, no harm is done in this case and at least in the early stages as an investigation can be started and the process can be transparent to normal every day business.

One of the most important steps in the initial phase of building such system is the collections of as much historical cases of deception as one can. The next most important step will be to link the knowledge base with existing stored protocols and existing system of network, database and communication securities.

The choice of an adequate ANN algorithm is very critical. In our case we will explore existing algorithms and attempt to use our own. Our own algorithm is base on the fact that an organization can be considered a biological being with dynamics that are space and time dependent. The dynamics will be modeled with distributed oscillations across the organization. These oscillations interact with each others in certain ways. The whole system of different entities (current employees, former employees, public, computer systems, networks, Internet… etc) is considered as an ensemble of behavior that either matches a normal one or matches or approaches a stored one. The matching mechanism will be critical here.

In figure 2 we represented potential elements of the whole system that can also be considered source of input to the ANN. Protocols must be set to help feed the knowledge base and the database of historical cases with real time data and fresh cases.

Input to the system may originate from the following sources:

- Network and database security logs (computer file containing records of attempted accesses to the system and record of areas, files, fields accessed when and by whom and for what purpose)
- Web browsing: Intra, Extra and Internet (Record of links and activities associated with web browsing)
- Emails: Intra, Extra and Internet (Record of all email transaction including messages their space and time stamps)
- Chats: Monitoring and recording of all chat transaction including messages
- Telephone: Monitoring and recording of all telephone transaction including messages.

All of these by taking into consideration issues of privacy. We assume that transactions associated with the mentioned resources are for the business of the organization and not for personal use.

But how the system would process input of linguistic nature? Natural language processing is critical in this case especially when all the processes are automated. A human expert in IT forensic would ask to have access to everything we listed above in order to conduct a thorough investigation. The expert may have no trouble reading and or listening to messages sent via email, chat and/or telephone conversation. The expert will be able to recreate past event from static information and infer what may have happened. In our case, the system should be able to do the same using static information such as a set of "recorded-everything" but the system should be able and in real time, raise an alert whenever an ongoing act of deception is ongoing.

One of the most important aspects of the research is mapping the environment depicted in figure 2 to one that is very similar to a semantic web. At least, and when mining for meaning, information stored as records, chat messages, phone conversations and emails' contents are all candidates for source of patterns than can be tested to check for those that match stored profiles of deception.

The mapping process by itself will be a major achievement. The semantics in this domain should be in a format that is usable by a machine. The machine in this case is our proposed system.

CONCLUSION

This paper presented some facts related to the human factor in IT security and proposed a system by which risks associated with deceptive activities that can compromise an organization security can be dealt with. The processes that the system will handle should be similar to those of a human expert. In this case, we acknowledge that the task is difficult as even with human expert errors of semantics can occur. In these cases the real meaning of knowledge may not be communicated properly. The success of such endeavor depends on many factors. Some of the most important factors consist of defining the different components of the problem domain, creating an exhaustive list of rules that can be used with the expert system dealing with the static nature of the knowledge base, building the collaborative interface between the expert system and the Fuzzy Neural Network and most importantly, the elements of the employee's environment presented in figure 5 must interface with the Fuzzy Neural Network in real time

There are available methodologies and technologies that can help model each part of the system. The only part that would require future work will be that of the Fuzzy Neural Network [1][9][17][18][19][23].

ACKNOWLEDGEMENTS

The initial phase of this work was partially funded by Frank Zarb School of Business at Hofstra University Hempstead New York in summer of 2003.

REFERENCES

[1]Abouzakhar, Nasser S; Manson, Gordon A, Networks Security Measures Using Neuro-Fuzzy Agents, Information Management & Computer Security; Volume 11 No. 1; 2003

[2]Aldridge, Alicia; White, Michele; Forcht, Karen, Security Considerations of Doing Business via the Internet: Cautions to be Considered, Internet Research; Volume 7 No. 1; 1997

[3]Baines, George, IT Security and Integrity, Work Study; Volume 39 No. 4; 1990

[4]Baskerville, Richard; Siponen, Mikko, An Information Security Meta-policy for Emergent Organizations, Logistics Information Management; Volume 15 No. 5; 2002

[5]Benn, David, Stopping the Rot of Disloyalty, Industrial Management and Data Systems; Volume 89 No. 5; 1989

[6]Chantry, John, Intruder Detectors: Myths of our Time, Facilities; Volume 16 No. 5; 1998

[7]Desai, Mayur S.; Richards, Thomas C.; von der Embse, Thomas, System Insecurity – Firewalls, Information Management & Computer Security; Volume 10 No. 3; 2002

[8]Dinnie, Garry, The Second Annual Global Information Security Survey

Information Management and Computer Security; Volume 7 No. 3; 1999

[9]Evans, D.J.; Tay, L.P., Fast learning artificial neural networks for continuous input applications, *Kybernetes; Volume 24 No. 3; 1995*

[10]Grossberg, S., Studies of the Mind and Brain, Drodrecht, Holland: Reidel Press, 1982.

[11]Harris, Geoffrey, Security and Fraud: Strategies for Prevention and Detection,

Logistics Information Management; Volume 4 No. 3; 1991

[12]Helms, Marilyn M; Ettkin, Lawrence P; Morris, Daniel J, Shielding your company against information compromise, Information Management and Computer Security; Volume 8 No. 3; 2000

[13]Higgins, Huong Ngo, Corporate system security: towards an integrated management approach, Information Management and Computer Security; Volume 7 No. 5; 1999

[14]Lee, Jintae; Lee, Younghwa, A holistic model of computer abuse within organizations, Information Management & Computer Security; Volume 10 No. 2; 2002

[15]Lichtenstein, Sharman; Swatman, Paula M.C., Internet acceptable usage policy for organizations, Information Management and Computer Security; Volume 5 No. 5; 1997

[16]Mitnick, K.D., Simon,W. L., The Art of Deception: Controlling the Human Element of Security, Wiley 2002.

[17]O'Leary, D.E., The Internet, Intranets, and AI renaissance, Computer, 30(1), pp. 71-78, January 1997

[18]Raggad, Bel G, Neural Network Technology for Knowledge Resource Management,

Management Decision; Volume 34 No. 2; 1996

[19]Rus , D.,Gray, R.,Kotz, D., Autonomous and Adaptive Agents that gather Information, AAAI '966 International Workshop on Intelligent Adaptive Agents, pp. 107-116, August 1996.

[20]Siponen, Mikko T, A Conceptual Foundation for Organizational Information Security Awareness, Information Management and Computer Security; Volume 8 No. 1; 2000

[21]Siponen, Mikko T, Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice,

Information Management and Computer Security; Volume 8 No. 5; 2000

[22]Smith, Alan D; Rupp, William T, Issues in Cybersecurity; Understanding the Potential Risks Associated with Hackers/Crackers, Information Management & Computer Security; Volume 10 No. 4; 2002

[23]Valentino, Christopher C , Smarter Computer Intrusion Detection Utilizing Decision Modeling, Kybernetes: The International Journal of Systems & Cybernetics; Volume 32 No. 5; 2003

[24]Warren G. K., Heiser, J.G., Computer Forensics: Incident Response Essentials, Addison Wesley 2002

[25]White, Gayle Webb; Pearson, Sheila J, Controlling Corporate E-mail, PC Use and Computer Security, Information Management & Computer Security; Volume 9 No. 2; 2001