6

Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security

Ines Brosso[1] and Alessandro La Neve[2]
[1]*Faculty of Computing and Informatics, Mackenzie Presbyterian University, Sao Paulo,*
[2]*Department of Electrical Engineering, Centro Universitário da FEI, SP, Brazil*

1. Introduction

At present, security policy, to be effective, is primarily focused on people, being very rigid at this, and only later it cares about security attack attempts.

The security policy does not need to be rigid: rather it should be adaptable to the user behavior.

Analysis of human behavior, therefore, is the basis for an adaptive security policy. The behavior analysis of a person can be verified by a set of rules, which consider the variables that can influence human behavior, based on the information acquired about the environment, space, time, equipment, hardware and software. This information is used to analyze behavioral evidences about people, and establishes if it is possible to believe or not in the user. Therefore, according to the user behavior, levels of trust are released, which are based on the rules that were previously established for the parameters that are necessary to establish the evidences of behavioral trust, in its different degrees.

The adaptive security policy based on user behavior analysis is the basis for the information security management, when it comes to understanding the needs of users.

However, to achieve the whole security target in computing, and related technologies, it is necessary not only to have the most updated core technologies or security policies, but also to have the capacity to perform the analyses of the user behavior and the security environment. This work, in the context of computer security, uses the operant and conditioning behavior defined by Skinner (1991), which rewards a response of an individual until he is conditioned to associate the need for action.

The Skinner Theory may be very interesting to be used in Information Security Management Systems. In operant behavior, the environment is modified and produces consequences that are working on it again, changing the likelihood of a future similar occurrence. Operant conditioning is a mechanism for learning a new behavior.

When the organism answers an environmental stimulation, and the consequences of its reply are rewarded, the probability of similar answers increases; when the consequences are punitive, such probability diminishes. People associate experiences they have gone through to similar ones they may find in life: in this case they adopt the same behavior and repeat their actions.

The methodology for the preparation of this book chapter consisted of literature review, research on historical, social and psychological aspects of the Behavioral Theory, and the development of an Intelligent Security System. Studies and research on mathematical methods for handling trust information, fuzzy-logic, Information security management, context-aware computing and adaptive security policies, were also necessary.

In order to integrate information security management, based on adaptive security policy, with user behavior analysis, a deep understanding of Behavioral Theory, with historical, social and psychological aspects are necessary. At the same time, it also important to have full expertise in mathematical methods for handling information about people behavior, context-aware computing and self-aware computing systems, which can be the basis for an adaptive security policy based on user behavioral analysis.

This work was based on a doctoral thesis (Brosso, 2006) and research in the area.

2. Adaptive security policy

One of the more challenging questions in security is how to specify an adaptive security policy. The security policy does not need to be rigid, but it should be adaptable to the user behavior. In this context, this work exploits security aspects, user behavior analysis, trust in behavior, and biometric technologies to be the base of an adaptive security policy. The goal for specifying adaptive security is twofold:

- to provide an umbrella guide to decide which future events, actions, or responses are permitted in the current policy; and
- to allow new security goals to be stated, in order to initiate system responses to enforce that policy, if necessary.

The security policies for computing resources must match the security policies of the organizations that use them; therefore, computer security policies must be adaptable to meet the changing security environment of their user-base. The term "adaptive security" is intended to indicate that security policies and mechanisms can change in some automated or semi-automated way in response to events.

3. USER behavior analysis

The user behavior analysis helps to define an adaptive security policy to the information security management. Human behavior is based on contextual information, which is retrieved by behavioral history, history of behavior reinforcement and conduct of the person to interact with the environment immediately (Witter, 2005).The scientific analysis of human behavior starts with the knowledge of the environment and isolation of the parts of an event to determine the characteristics and the dimensions of the occasion where the behavior occurs, and to define the changes that were produced in response to the environment, space, time and opportunities.

The user behavior is a combination of n dimensions. The user behavior analysis uses the context variables of the environment and the trust, the concept that we human beings have regarding a person, and it is based on the behavior and reputation of a person. In this way, the environmental variables model of the user's behavior, in a conditioning process, uses the concepts of user, context, environment, time interval, behavior and trust, as follows:

- **User -** User is a person who has been approved in an authentication process to have access to software applications in a specific area of computer networks and wireless.
- **Context -** Any information that can be used to characterize the situation of the environment and the user.
- **Environment –** *Environmental technology*: the infrastructure needed in a specific area of computer networks, wired and wireless. *Technological environment:* local capture information, from behavior of users that interact with software and hardware applications.
- **Time interval -** The interval of time that elapses from the initial instant the user makes his identification on a software application access to the moment he exits the application, often called the session.
- **Behavior** - The behavior is the set of actions and responses that enable the intent of a person and the technological environment; or actions that a user performs when interacting with the software applications and the technological environment.
- **Trust** - Concept assigned to the user, which may vary according to the behavioral analysis of it. Based on the evidence of user behavior it is possible to determine the level of trust to give him. Trust is an abstract concept that expresses the belief that one has in the sincerity or authenticity of another person. The trust level of the person user is according to the analysis of his behavior. The concept of trust is a characteristic common to human beings, and is directly related to the perception, knowledge and reputation of a person about another. *Trust Restriction* -It refers to the behavior of the user that runs off the expected normality. A restriction may be due to a sequence of not recommended transactions, values or places different from usual, or others. The restriction of trust can be used in user adaptive security policy.

The focus of Behavior Analysis, as proposed by Skinner (1991), is currently applied in this work, for effective analysis of user behavior, to fulfill the requirements of user behavior analysis, according to the following steps:

Behavioral analysis is based on evidence of user behavior and comparison with information stored in databases of the same behavioral history. The behavioral analysis is carried out in two phases:

- The first is to compare the information obtained at the time the user interacts with the historical behavioral information.
- The second phase is to verify the existence, or absence, of behavioral constraints that can collaborate with the analysis, to convey or not to the user authentication.

The capture of user behavioral information in the environment is done analyzing some human elements of information security. It is closely associated with such characteristically human activities as philosophy, science, language, mathematics and art, and is normally considered to be a definitive characteristic of human nature. Human nature refers to the

distinguishing characteristics, including ways of thinking, feeling and acting, that humans tend to have naturally.

Steps of analysis of user behavior	Description
Step 1: Target of the Behavior	Define the target of the behavior to be analyzed, to measure the frequency with which it occurs, or capture the variable and compare it with the restrictions and historical behavior in databases.
Step 2: Observe the behavior	Observe the behavior, the response and what will happen, or wait for the action of the user interaction in a given period of time, capturing the information received and waiting for the application to send a stimulus to the user to develop his behavior.
Step 3: Observe the behavior in terms of triple contingency	Observe the behavior in terms of triple contingency, which is the expression used to say that it will see the context, the response and what will happen; or wait for the action of the user interaction with the application software in a given period of time, capture the information received and wait for the application to send the user a stimulus to provoke a certain behavior.
Step 4: Behavior frequency	Record the rate of occurrence of the behavior, (frequency), in order to measure the behavior occurred throughout the process, and stores it in the user behavior database.
Step 5: Introduce the experimental variable	Where appropriate, introduce the experimental variable. It is applied to introduce a new tool for the user, such as a new code of access or a new field of application.
Step 6: Compare the frequency of behavior	Compare the frequency of behavior before and after the experimental variable or the occurrence of response. Currently, restrictions are compared to the user's past behavior. Thus, it can be said that the environment and both the virtual and physical space establish the conditions for a certain behavior.

Table 1. Steps of analysis of user behavior

The questions concerning these characteristics, what causes them and how this causation works, and how fixed human nature is, are amongst the oldest and most important questions in western philosophy. These questions have important implications particularly in ethics, politics and theology.

The user behavior analysis will also be concentrated on understanding how we can trust in the user.

In this work, relevant human elements like reason, logic and trust, are used in this study.

4. Human elements

Some Human Elements like reason, logic and trust help to analyze both the user behavior and to study a source of norms of conduct or ways of life to produce an adaptive security policy.

5. Reason

Beer (1994) explains that reason is a term that refers to the capacity that human beings have to make sense of things, to establish and verify facts, and to change or justify practices, institutions and beliefs. The concept of reason is sometimes referred to as rationality and was considered to be of higher stature than other characteristics of human nature. Reason is associated with thinking, by which it flows from one idea to a related one. It is the means by which rational beings understand themselves thinking about truth and falsehood, and what is good or bad. Reason relies on mental processes, related to the primary perceptive ability of humans, which gathers the perceptions of different senses and defines the order of the things that are perceived. Reasoning, in an argument, is valid if the argument's conclusion comes to be true when the premises, or the reasons given to support that conclusion, are true. If such reasoned conclusions are originally built only upon a foundation of sense perceptions, on the other hand, conclusions reached in this way are considered more certain than sense perceptions on their own.

Gilovich (1991) explains that psychologists and cognitive scientists have attempted to study and explain how people reason, what cognitive and neural processes are engaged, and how cultural factors affect the inferences that people draw to determine whether or not people are capable of rational thoughts in various different circumstances.

Experiments investigate how people make inferences about factual situations, hypothetical possibilities, probabilities, and counterfactual situations, and how it influences the human behavior. Humans have certain invariant structures, such as coherence and ability to establish relationships that give rise to the categories of reason that are structured in touch with reality, so that reason becomes a result of the action of biological maturation and the environment. Reason is a consideration that explains or justifies some behavior of humans in the field of logic.

6. Logic

Gottwald and Hajek (2005) wrote that, in contrast with traditional logic theory, where binary sets have two-valued logic, true or false, fuzzy logic variables may have a truth value, that ranges in degree from 0 to 1. In logic, a many-valued logic or multi-valued logic is a propositional calculus in which there are more than two truth values.

Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact and it has been extended to handle the concept of partial truth, where the truth value may range from completely true to completely false. While variables in mathematics usually take numerical values, in fuzzy logic applications, the non-numeric linguistic variables are often used to facilitate the expression of rules and facts.

Logical systems in general are based on some formalized language which includes a notion of well-formed formula, and then they are determined either semantically or syntactically. A logical system that is semantically determined means that one has a notion of interpretation or model, each such interpretation every well-formed formula has some (truth) value or represents a function into the set of (truth) values. It means, furthermore, that one has a notion of validity for well formed formulas and, based upon it, also a natural entailment relation between sets of well formed formulas and single formulas (or sometimes also whole sets of formulas).

That a logical system is syntactically determined means that one has a notion of proof and of provable formula, i.e. of (formal) theorem, as well as a notion of derivation from a set of premises. From a philosophical, especially epistemological point of view, the semantic aspect of (classical) logic is more basic than the syntactic one, because semantic ideas mainly determine what are suitable syntactic versions of the corresponding (system of) logic.

Fuzzy set theory defines fuzzy operators on fuzzy sets. The problem in applying this is that the appropriate fuzzy operator may not be known. For this reason, fuzzy logic usually uses IF-THEN rules, or constructs the equivalent ones, such as fuzzy associative matrices. There are also other operators, more linguistic in nature, called hedges that can be applied. These are generally adverbs such as "very", or "somewhat", which modify the meaning of a set using a mathematical formula.

Zadeh (1968) proposed that in mathematical logics, there are several formal systems of "fuzzy logic"; most of them belong to the so-called t-norm fuzzy logics. The notions of a "decidable subset" and "recursively enumerable subset" are basic ones for classical mathematics and classical logic. Ω denotes the set of rational numbers in [0,1]. A fuzzy subset $s : S \rightarrow [0,1]$ of a set S is recursively enumerable, if a recursive map $h : S \times N \rightarrow \Omega$ exists such that, for every x in S, the function h(x,n) is increasing with respect to *n* and s(x) = lim h(x,n); *s* is decidable if both *s* and its complement –*s* are recursively enumerable. An extension of such a theory to the general case of the L-subsets is proposed in Gerla (2006).

One of the main interests of the fuzzy logic theory is that many parameters can be taken into account since no mathematical modeling is required. This applies to the plant control area, but also to forecasting, decision support and risk scoring. On the other hand, Ang (2003) refers to neuro-fuzzy as combinations of artificial neural networks and fuzzy logic, the Neuro-Fuzzy Logic Rules and fuzzy sets are optimized by training strategies originated from neural network theory. In logic, trust is a dimensional, or multidimensional, variable, because it is possible to trust, not trust or have no evidence to attribute trust over an interval of time.

7. Trust

Trust is an abstract concept, and it reveals a belief in the sincerity or authenticity of one person in relation to another. Trust, a concept that we human beings have regarding a person, is based on the behavior and reputation of a person. This concept is not a unique and indivisible attribute that can be given to someone, and it is not the dichotomy of trust or not trust: on the contrary, it can be graded, and therefore it is dimensional and measurable. Trust levels may be stipulated based on the user behavioral analysis and on trust restrictions

generated by the user. Trust level of the user is given according to the analysis of his behavior.

According to the user behavior, trust levels are released, to let the user have access to the application software. These levels, however, are not determined by clear and cut rules, that reflect a classification that can easily and universally be applied to human actions, but rather they must reflect the shady, undefined, and yet evident, characteristics of human behavior. With the increase of behavior information, a more efficient support for behavior evidences analysis is generated, and the system continues performing the evidences analysis of the behavior and adjusting the trust in the user.

Trust can change depending on the user, the localization, the time and the trust restrictions. With trust based on behavioral information and in the environment context information, it is possible to infer a minimum value for the initial trust, and, along the time, based on the behavior analysis and in the trust restrictions, the system will change the levels of trust.

The heuristics adopted to define the initial trust can be defined according to the user activity at a particular moment, its location, the time that the behavior currently occurs, and his historical behavior.

The attribution of the subsequent levels of trust is processed in two stages:

- 1st stage – Since there is not enough behavior information, it is attributed a minimum level of trust and, at the end, it accounts and stores the captured information.
- 2nd stage - In the subsequent accesses, when the user interaction increases, a verification is done, at first, in the trust restrictions database: if there are no restrictions, it compares the current behavior with the behavior information database, but if there are any changes in behavior, the alarm is triggered, the new behavior is stored, trust is re-calculated and security mechanisms are trigged.

According to the user behavior, levels of trust are released, based on the rules that were previously established for the parameters which help to establish the evidences of behavioral trust, in its different degrees.

Thus, it can be said that the environment and both the virtual and physical space establish the conditions for a certain behavior. It is necessary, therefore, to define some entities, used in behavior analysis, a set of context variables *{who, where, when, what, why, how, rest}*, that is, the evidence of the user behavior, as in table 2.

The set of context variables *{who, where, when, what, why, how, rest}* helps to decide what information is relevant to a system. However it is necessary to analyze the requirements and model the necessary information that each dimension can provide, since, in general, there is a tendency to develop a context model in which the user overrides associated problems, and this is a generalization to classify the context in temporal aspects, both static and dynamic.

To capture the behavior means to store the information of the behavioral variables *{who, where, when, what, why, how and rest}*, in a data structure represented by the matrix of user behavior. Given the uncertainty and doubt, it is often necessary to take decisions based on

evidences, which are not always accurate. In these cases, trust should be used, which is a staff metric criterion adopted to evaluate evidence.

Variables	Description
Who	Identification. It identifies the user in an application software session. It helps User-behavior analysis, in classifying users according to their access patterns. This is useful for personalization, targeted advertising, priority, and capacity planning.
Where	Space Locality: It identifies either the location where the user is, or the device address that the user is accessing. It is of user interest, determining whether users in the same geographical region tend to receive or request similar notification and browsing content. For analysis, it should be defined a notification message to be locally shared, if at least two users in the same cluster receive the notification.
When	Time. It identifies the current time that the user is in a software application session.
What	Qualification. It identifies what the user is doing in a software application session.
Why	Intention. It means the action of the user to the stimulus received.
How	Method. It justifies the user repetitive activities in a software application session.
Rest	Restrictions. It identifies either the user behavior or the software application restrictions.

Table 2. Variables of the evidence of the user

The concept of trust is a characteristic common to humans, and is directly related to perception, knowledge and reputation that a person has about the other. According to Dempster (1967) and Shaffer (1976), a measure of confidence, in a universe set X that represents the total amount of confidence in the evidence of a particular set of circumstances, which varies between 0 and 1, is given by the function: Cf (x): P (X) ← [0, 1].

Based on the evidences of the behavior, the application software establishes if it trusts the user with values in the interval (mC, mD), where mC is the initial minimum trust and mD is the initial minimum diffidence.

The confidence (Cf), the diffidence (Df) and the uncertainty (If) express all the possibilities of trust attribution to a user, in this form:Cf + Df + If = 1. The uncertainty If is defined as: (If) = 1- (Cf + Df).

If Bj is a user behavior, the System, based on the evidences of the behavior, establishes if it trusts the user with values in the interval (mC, mD), where mC is the initial minimum trust and mD is the initial minimum diffidence. The system checks the uncertainty of confidence, which is given by: If (Bj) = 1 - (mC + mD). If the behavior Bj is considered normal, confidence is assigned to the user, linearly and slowly.

If there is uncertainty, safety mechanisms, like sensors that capture the user information, can be triggered and compare it with the existing one in databases. If there is an unusual behavior, behavioral constraints are generated, decreasing the confidence and increasing

distrust. If there are any differences, confidence in the user will be decreased, and even access and continuity of operation are liable to be blocked. In case of indications of changes, in the user's behavior, if there are uncertainties and divergences, security mechanisms and alert signals are triggered.

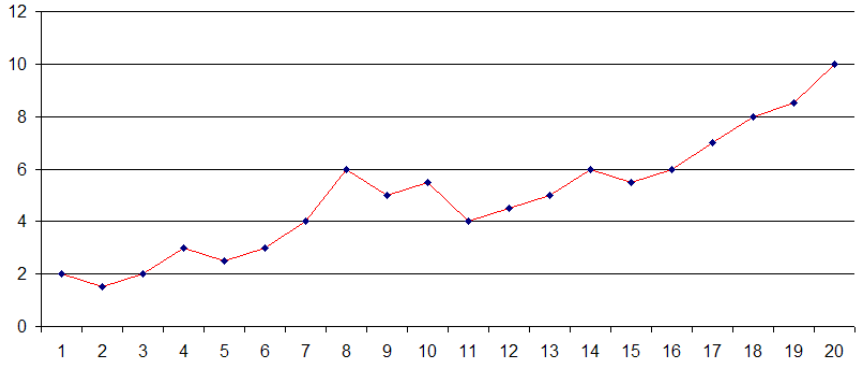


Fig. 1. The increase of trust

The loss of confidence grows fast, as it can be seen in figure 2.

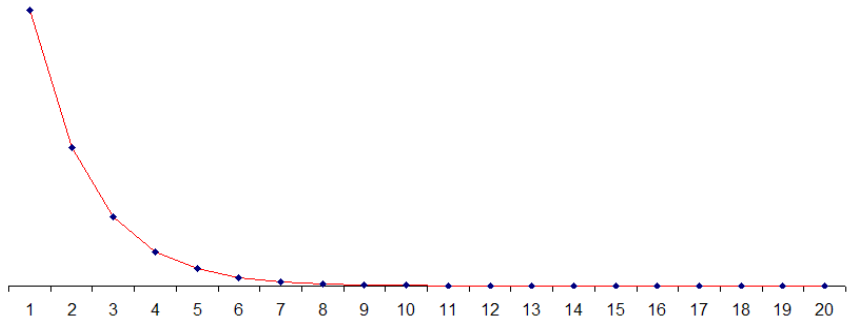


Fig. 2. The loss of trust

There is an uncertainty in the allocation of trust, however, because not always the complement of the expressed trust is distrust. Along the time, and in accordance with the behavior analysis, the user trust level can be subject to variations, and thus, it is necessary to interact with the user, to determine evidences so as to increase or to decrease trust in the user. Considering the definitions of reason, logic and trust, we can see that people use logic, deduction, and inductions, to reach conclusions that they think are true.

8. The information security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection,

recording or destruction. The terms information security, computer security and information assurance are often interrelated and share the common goals for protecting the confidentiality, integrity and availability of data regardless of the form the data may take electronic, print, mobile or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures. Governments, military corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted to other computers across networks.

Should confidential information about a business customer, or a new product line, fall in the hands of a competitor, such breach in security could lead to losses in business, law suits or even bankruptcy of companies. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

Information Security is composed of three main parts, namely hardware, software and communications, to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Procedures or policies are essentially implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

The field of information security has many areas including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, digital forensics science, security systems, etc. In this work we study an intelligent security system in collaboration with the information security.

9. An intelligent security system

It is here presented a study about an intelligent security system that uses an adaptive security policy using User Behavior Analysis and Human Elements of Information Security.

Figure 3 shows the mechanism that is used when the user accesses the computer: the intelligent security system verifies and analyzes the user behavior. This system is based on the fuzzy logic theory and must be able to acquire information about the environment, space, time, equipment, hardware, software and user behavior analysis, established for the variables *{who, where, when, what, why, how, rest}*. Fuzzy logic considers truth values, that are a value indicating the relation of a proposition to truth, ranging from 0 to 1 – but conceptually distinct, due to different interpretations.

The intelligent system proposes that, based on the evidences of the user behavior, it is possible to trust or not trust the user. Levels of trust are released, according to the user behavior and the rules that were previously established for the parameters which help to establish the evidences of behavioral trust, interacting with the environment information, so as to keep trust levels updated.

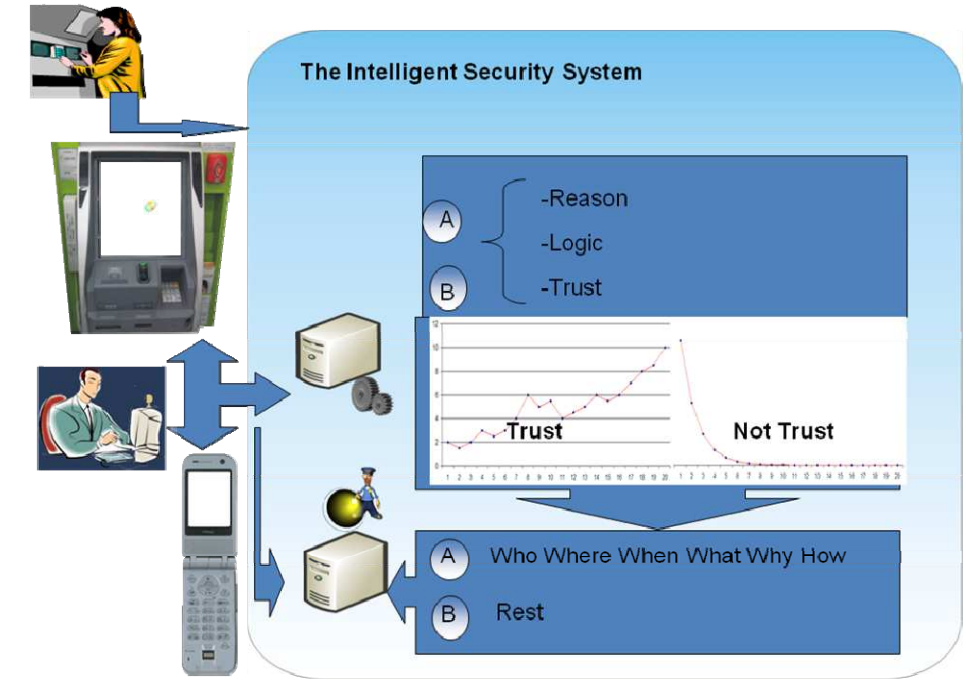


Fig. 3. The Intelligent Security System

The intelligent security system should be prepared not to anticipate every possible action that may be taken in the future, but to be flexible enough to adapt itself more easily to the changes that will certainly come, identifying technological trends and knowing more about human behavior, which will always be the crucial aspect of security.

Neural networks are systems that try to make use of some of the known or expected organizing principles of the human brain. Neural networks can be used if training data is available. It is not necessary to have a mathematical model of the problem of interest, and there is no need to provide any form of prior knowledge.

The neural function system has to learn what the behavioral changes of the user are, and incorporates them in the system, for a future fuzzy treatment. The fuzzy system evaluates, within an historical and behavioral perspective, human behavior, reflecting the perception or feeling that man or society have in relation to behavioral attitudes. Based on these attitudes weights are qualified and assigned.

On the other hand the solution obtained from the learning process usually cannot be interpreted. Neural networks and fuzzy systems have certain advantages over classical methods, especially when vague data or prior knowledge are involved. However, their applicability suffered from several weaknesses of the individual models. Therefore, combinations of neural networks with fuzzy systems have been proposed, where both models complement each other.

The proposed intelligent system adopts neuro-fuzzy logic because of its capacity to use past experiences and learn new ones. Weights can be attributed in the fuzzyfication process, according to the rules that were previously established for the variables {*who, where, when, what, why, how, rest*}, which help to establish the evidences of behavioral trust, in its different degrees.

The fuzzyfication of qualifiers should consider the intrinsic characteristics of the variables, according to specific application in which they are used. A financial institution, for instance, might consider the depositor of a bank for the variable *who*. Some qualifiers that could be associated to this variable might be: new or ancient (client), young or aged (person) , and others that the financial institution might find interesting or important in order to better define their clients.

A neuro-fuzzy system can feed the user behavioral database continuously, interacting with the fuzzyfication mechanism, so as to keep trust levels updated according to the user behavior, in a more accurate and faithful way, and to give more robustness to the system based on user behavior. The fuzzy set theory, as used here ,is based on if-then rules. The antecedent of a rule consists of fuzzy descriptions of input values, and the consequent defines a possibly fuzzy output value for the given input. The benefits of these fuzzy systems lie in the suitable knowledge representation.

According to the user behavior, levels of trust are released, to have access to the application software. These levels, however, are not determined by clear and cut rules, that reflect a classification that can easily and universally be applied to human actions, but rather they must reflect the shady, undefined, and yet evident, characteristics of human behavior.

In fact a major difficulty arises when actual values must be attributed to the parameter "*m*"(minimum), which is used in the Cf(x) and Df(x) functions, because of the subjectivity involved. Since there are no behavioral rules that can strictly be applied to people, no matter what their personal characteristics are, a more suitable mathematical tool, like soft-computing, should be used. The adoption of fuzzy logic, as a way of thinking, and then subsequently neuro-fuzzy systems, with learning possibilities, turned out to be a very interesting and effective solution.

Fuzzy logic allows that weights be attributed, based both on the designer's system needs and the experience drawn from historical events. With this in mind, and at hand, fuzzyfication rules, which are necessary to quantify vague and undefined qualifications, can be implemented resorting to the user behavior database, so as to find the optimal solution in each case, or set of cases.

The dynamism with which users access the system, constantly requires that the authentication system, as mentioned before, continuously revise, and possibly recalculate, trust levels to be released to the user, based on the behavioral history that the user himself continuously builds.

Neural networks are systems that try to make use of some of the known or expected organizing principles of the human brain. They consist of a number of independent, simple processors: the neurons. These neurons communicate with each other via weighted connections.

The modeling of single neurons and the called "learning rules" for modifying synaptic weights can be used in neural networks if training data are available. It is not necessary to have a mathematical model of the problem of interest, and there is no need to provide any form of prior knowledge. On the other hand the solution obtained from the learning process cannot usually be interpreted.

Although there are some approaches to extract rules from neural networks, most neural network architectures are black boxes. The fuzzy set theory makes possible that an object or a case belong to a set only to a certain degree that includes similarity, preference, and uncertainty.

The idea of combining fuzzy systems and neural networks is to design an architecture that uses a fuzzy system to represent knowledge in an interpretable manner and the learning ability of a neural network to optimize its parameters.

A combination can constitute an interpretable model that is capable of learning and can use problem-specific prior knowledge. Neural networks and fuzzy systems have established their reputation as alternative approaches to information processing.

Neuro-fuzzy models are neural networks with intrinsic fuzzy logic abilities, where the weights of the neurons in the network define the premise and consequent parameters of a fuzzy inference system. Premise parameters determine the shape and size of the input membership functions, whilst consequent parameters determine the characteristics of the output, exemplified in Figure 4.

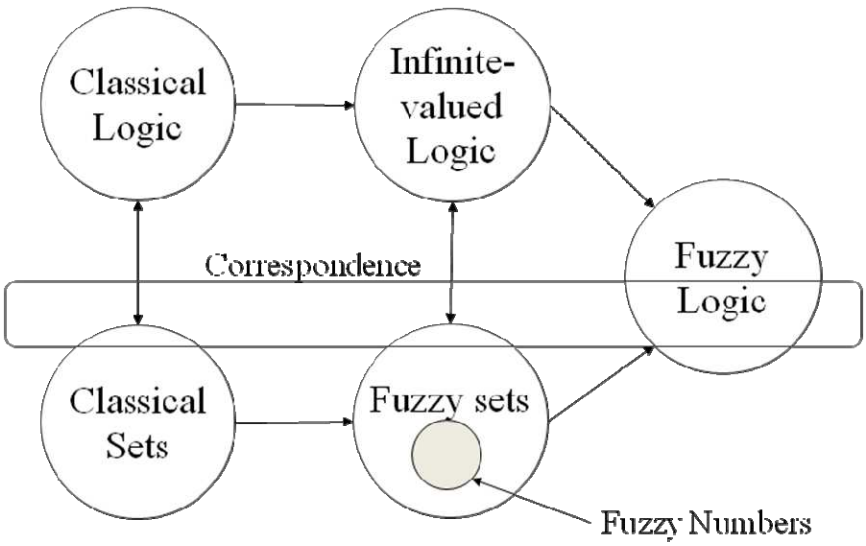


Fig. 4. The structure of Fuzzy Logic

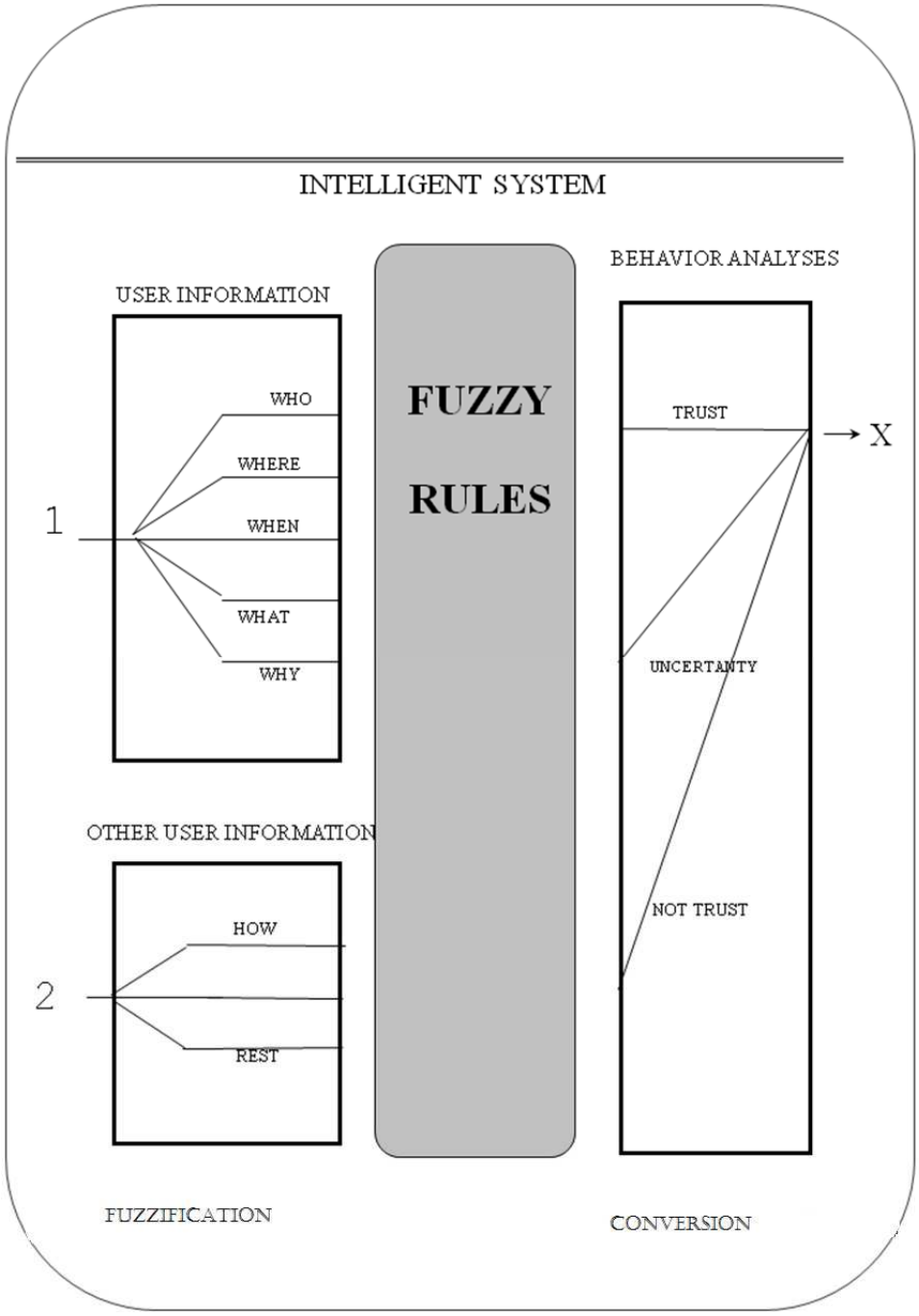


Fig. 5. The architectural of the Intelligent Security System with variables

It is therefore necessary to count on a mechanism with learning ability, such as a neuro system, that is able to give support to the fuzzyfication rules, according to the user behavioral changes. This will, not only update the user behavioral database, but it will interact with the fuzzyfication mechanism, so as to keep trust levels updated ,according to the user behavior, in a more accurate and faithful way.

With the increase of behavior information, a more efficient support for behavior evidences analysis is generated, and the system continues performing the evidences analysis of the behavior and adjusting the trust in the user. The trust can change depending on the user, the localization, the time and the trust restrictions.

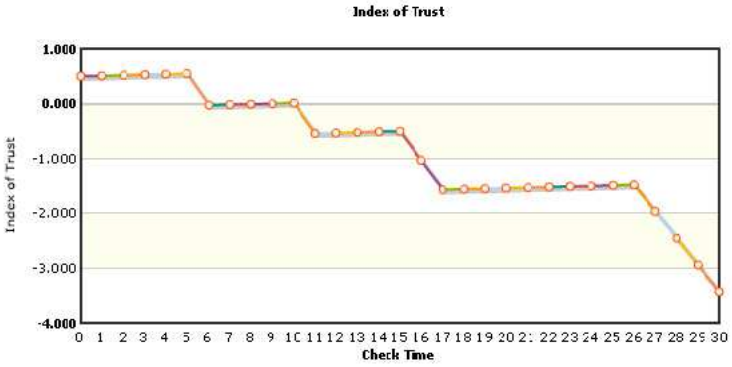
Date / Time	Trust	Untrust	Index of Trust
05/11/2009 08:48:15	0,56	0,576949810380487	-0,0169498103804869
05/11/2009 08:48:05	0,55	0,576949810380487	-0,0269498103804869
05/11/2009 08:47:58	0,55	0	0,55
05/11/2009 08:47:33	0,54	0	0,54
05/11/2009 08:47:26	0,53	0	0,53
05/11/2009 08:47:16	0,52	0	0,52

Fig. 6. Trust variation.

The system attributes trust based on behavioral information and in the context information from the environment, and so, it is possible to infer a minimum value for the initial trust, and along the time the system will change the trust, based on the behavior analysis and in the trust restrictions.

For the Intelligent System, "behavior" is the action of the user to the stimulus received, and "to capture the behavior" means to store the information of behavioral variables (*who, where, when, what, why and rest)* in a data structure represented by the matrix of user behavior.

The human behavior is uncertain and unpredictable. It is not algorithmic. It is based on the individual history of the person and groups. Therefore, the individual experience of the person should be considered in this analysis. The greater the amount of captured information, the better the analysis behavior will be. The user behavior is a combination of *n* dimensions. The focus of Behavior Analysis proposed by Skinner (2003) is currently applied to the system for effective analysis of user behavior according to the steps that were defined in table 1.



Add Trust Add Untrust

Date / Time	Trust	Untrust	Index of Trust
05/11/2009 08:50:08	0,72	4,14346972096867	-3,423-6972096867
05/11/2009 08:50:06	0,72	3,6567174650087	-2 9367174650087
05/11/2009 08:50:03	0,72	3,16996520904873	-2,44996520904873
05/11/2009 08:49:56	0,72	2,68321295308876	-1,96321295308876
05/11/2009 08:49:48	0,72	2,19646069712879	-1,476-6069712879
05/11/2009 08:49:45	0,71	2,19646069712879	-1,486-6069712879

Fig. 7. Trust variation with trust restrictions.

10. Conclusion

To establish the policy and mechanisms for an adaptive security system, which is intended to protect society and its institutions, it is fundamental to know and analyze more deeply, besides the different technical and organizational aspects of the system, human behavior, which is often neglected.

Human behavioral characteristics, in fact, are some very important components that have to be considered, since they are partly subjective , but they are also strongly influenced by the social group the individuals belongs to: they may be predictable, to a certain extent, but they are certainly not ascertainable algorithmically.

Therefore, the need of mathematical support, in the design of an adaptive security system, conveys to the adoption of a neuro-fuzzy system. Neuro-fuzzy systems have the necessary flexibility to use past experiences, which are not algorithmic, and learn new ones. The neuro-fuzzy system allows that the user behavioral database be continuously updated, interacting with the fuzzyfication mechanism, so as to keep trust levels updated ,according to the user behavior, in a more accurate and faithful way.

The implemented Intelligent System was validated with tests and simulations to authenticate a person's identity using behavior analysis and trust restrictions, which are the basis for an adaptive security system. It acquired information in the context that was submitted, and they were used as a basis for user behavior. The System, based on the evidences of the user behavior, established if the user could be trusted or not, and to what extent.

So, according to the user behavior, levels of trust were released, to access the application software. Weights were attributed in the fuzzyfication process, according to the rules that were previously established for the parameters *(who, where, when, what, why, rest)*, which help to establish the evidences of behavioral trust, in its different degrees.

Therefore, with this approach, it was possible to define an adaptive security policy, based on the behavioral analysis of computer network users.

In future developments, the intelligent system for information security should be prepared, not to anticipate every possible action that may be taken, but to be adaptable enough to respond more rapidly to the changes that will certainly come. It should also be capable of identifying new technological trends and know more about human behavior, which will always be the crucial aspect of a security system.

Besides this, considering the steady and fast evolution of Information Technology and Communications in its manifold aspects, which are becoming more complex and sophisticated, it is necessary to think of a larger System, a Security Management System, that is not only robust enough to correspond to the current needs, but it may also be intelligent and prepared for the future, so as to guarantee to society the real benefits that Information Technology has to offer.

11. References

Ang, K. K., Quek, C., & Pasquier, M. (2003). "POPFNN-CRI(S): pseudo outer product based fuzzy neural network using the compositional rule of inference and singleton fuzzyfier." IEEE Transactions on Systems, Man and Cybernetics, Part B, 33(6), 838-849.

Azzini, A.; Marrara, S.; Sassi, R.; Scotti, F. (2007) A fuzzy approach to multimodal biometric authentication. In *Proceedings of the 11th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, KES'07*, Vietri sul Mare (SA), Italy, September.

Beer, Francis A., "Words of Reason", Political Communication 11 (Summer, 1994): 185-201.

Brosso, I. (2006) *Users continuous authentication in computers networks* – Doctoral Thesis in Digital Systems at Polytechnic School of Sao Paulo University, Brazil, from http://www.teses.usp.br/teses/disponiveis/3/3141/tde-08122006-170242/en.php

Brosso, I,; La Neve, A.; Bressan, G.; Ruggiero, W.V. (2010) A Continuous Authentication System Based on User Behavior Analysis, *International Conference on Availability, Reliability and Security, International Conference* , pp. 380-385, Krakow, Poland, February 15-February 18, ISBN: 978-0-7695-3965-2, retrieved December 2010 from http://doi.ieeecomputersociety.org/10.1109/ARES.2010.63

Dempster, A. P. (1967) Upper and Lower Probabilities Induced by a Multi-valued Mapping, *Annals of Mathematical Statistics*, Vol.38, pp.325-339.

Gerla, Giangiacomo (2006). "Effectiveness and Multivalued Logics". Journal of Symbolic Logic 71 (1): 137–162. doi:10.2178/jsl/1140641166. ISSN 0022-4812.

Gilovich, Thomas (1991), How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life, New York: The Free Press, ISBN 0-02-911705-4

Gottwald, S., and Hajek, P. (2005). T-norm based mathematical fuzzy logics. In: Logical, Algebraic, Analytic, and Probabilistic Aspects of Triangular Norms (E.P. Klement and R. Mesiar, eds.), Elsevier, Dordrecht, 275-299

Hájek, Petr (1998). Metamathematics of fuzzy logic. Dordrecht: Kluwer. ISBN 0792352386.

Nauck, D.; Klawonn, F.; and Kruse, R. ; (1997) Foundations of Neuro-Fuzzy Systems, Wiley, Chichester.

Nurnberger, A. (2001) A Hierarchical Recurrent Neuro-Fuzzy System, In Proc. of Joint 9th IFSA World Congress and 20th NAFIPS International Conference, pp. 1407-1412, IEEE.

Platzaer, C (2004) Trust-based Security in Web Services. Master's Thesis – Technical University of Vienna, May.

Shaffer, G. (1976) *A Mathemathical Theory of Evidence*. Princeton, Princeton University Press.

Skinner, B.F. (1991). The Behavior of Organisms. p. 473. ISBN 0-87411-487-X. Copley Pub Group.

Truong, K.N.; Abowd, G.D.; Brotherton J.A. (2001) *Who, What, When, Where, How: Design Issues of Capture & Access Applications*. Georgia Institute of Technology

Technical Report GIT-GVU-01-02. January. York, J.; Pendharkar, P.C.(2004) *Human–computer interaction issues for mobile computing in a variable work context*, Int. J. Human-Computer Studies 60 ,771–797.

Weiser; M.; Gold, R.; & Brown, J. S. (1999) *Ubiquitous computing* - Retrieved 9 December 2010 from http://www.research.ibm.com/journal/sj/384/weiser.html.

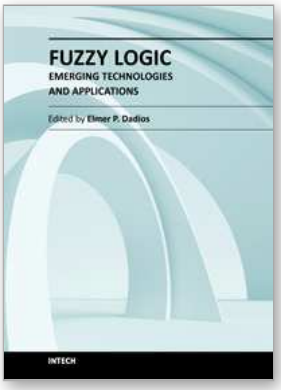
Witter, G.P. (2005) *Metaciência e Psicologia*, (Portuguese language) ISBN: 8575161075 , São Paulo, Brazil. Editora: ALINEA

Zadeh, L.A. (1965). "Fuzzy sets". Information and Control 8 (3): 338–353. doi:10.1016/S0019-9958(65)90241-X. ISSN 0019-9958.

Zadeh, L.A. (1968). "Fuzzy algorithms". Information and Control 12 (2): 94–102. doi:10.1016/S0019-9958(68)90211-8. ISSN 0019-9958.

Zemankova-Leech, M. (1983). Fuzzy Relational Data Bases. Ph. D. Dissertation. Florida State University.

Zimmermann, H. (2001). Fuzzy set theory and its applications. Boston: Kluwer Academic Publishers. ISBN 0-7923-7435-5.



Fuzzy Logic - Emerging Technologies and Applications

Edited by Prof. Elmer Dadios

ISBN 978-953-51-0337-0
Hard cover, 348 pages
Publisher InTech
Published online 16, March, 2012
Published in print edition March, 2012

The capability of Fuzzy Logic in the development of emerging technologies is introduced in this book. The book consists of sixteen chapters showing various applications in the field of Bioinformatics, Health, Security, Communications, Transportations, Financial Management, Energy and Environment Systems. This book is a major reference source for all those concerned with applied intelligent systems. The intended readers are researchers, engineers, medical practitioners, and graduate students interested in fuzzy logic systems.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821