SKETCH OF A GENERIC SECURITY FRAMEWORK BASED ON THE PARADIGMS OF SYSTEMIC-HOLISTIC APPROACH AND THE IMMUNE SYSTES

Jeffy Mwakalinga, Louise Yngström

Department of Computer and System Sciences

Royal Institute of Technology / Stockholm University

Forum 100,

S-164 40 Kista, Sweden

Email: jeffy@dsv.su.se, louise@dsv.su.se

Tel: +468 161 721

Fax: +468 703 90 25

ABSTRACT

Everything that we see can be changed. Internet is vulnerable because it was not designed as a whole system. This can be changed by changing the way we think and approach the development of Internet. Initial development of the Internet and other systems focused only on computer technology and communication's protocols. Many systems are not secure today because most research has concentrated on securing parts of the systems. Hence, we can change this by viewing security of Internet and other systems holistically, by focusing not just on technology and protocols but by considering system's environments, people using the systems, future of systems and other factors. In this paper we view and approach security of systems holistically. We discuss and suggest a methodology of securing systems based on the paradigms of the Immune system and the Systemic-Holistic approach. The Immune system is used to protect human bodies from for instance different types of viruses. The Systemic-holistic approach views and studies a system as a whole or in details at the theoretical, design, or the implementation level. It takes into considerations technical and non-technical aspects and the system's environment. The generic security framework has been created for using functions inspired by the immune system and the systemic-holistic approach paradigms to secure systems. The framework contains the deterrence, protection, detection, response and recovery sub-systems. These sub-systems will be generically protecting both at the border and internally in the system. This methodology will improve the way we design security systems by generically considering different factors and people using the system.

KEY WORDS

Immune system, Systemic-holistic, negative selection algorithm, clonal selection algorithm, deterrence, protection, detection, response, recovery, intrusion detection, software agents and generic security framework.

SKETCH OF A GENERIC SECURITY FRAMEWORK BASED ON THE PARADIGMS OF SYSTEMIC-HOLISTIC APPROACH AND THE IMMUNE SYSTES

1 INTRODUCTION

This paper describes a generic security framework aimed for sorting in functions inspired by the immune system and the systemic-holistic approach paradigms useful to secure systems. Internet and computers are vulnerable because of the assumptions initially directing the developments of computers and communications protocols. In addition it was overlooked that users have various reasons for communicating. To handle the security problems it has been assumed that all systems, static and dynamic, can be correctly verified with formal methods. [See for instance 1]. To formally verify that a static system does what it is supposed to do, is expensive; to formally verify that dynamic systems are correctly implemented with formal verification methods is impractical [1]. In addition it has been assumed that: security policies can be performed and followed perfectly; that programs, large and small, can be perfectly implemented; and that systems can be perfectly configured [1]. But all these assumptions are not correct [1]. Conclusions to be drawn are that formal verification methods for systems are not enough and other or complementary methods are sought for [1, 2]. It is challenging to verify that static and dynamic systems are secure with the current technology. So we have to find other ways of designing security systems by generically considering as many factors as possible. This includes studying how nature protects natural living systems.

In this work we discuss a framework based on the mentioned paradigms which eventually would inspire an adaptability view on securing systems. We do this because we think time might be ripe for marrying the Systemic-holistic approach, which has been used with us as a base to understand security in relation to IT since the mid-1980's [2], with the Immune system paradigm [1, 14]. Also, some other scientific paradigms/approaches are appearing to underline needs for including nature-oriented views into traditional engineering fields [11]. The Systemic-holistic is based on the General living Systems Theory [16, 8, and 2], Cybernetics [17, 10] and General Systems Theory [16, 15, and 2]. The approach is used for studying, investigating, designing security systems, analyzing security systems; in three dimensions of a system as one whole system as discussed in section 2.1. The human's immune system is distributable, multi-layered, autonomous, adaptable, dynamic, which seems very attractive to security systems. A number of researchers [3, 1, and 9] have developed computer security systems based on Immune systems. But the human's immune system can't be directly applied to computer systems because human bodies are made of cells, most of which are created in the bodies, while computers consist of hardware and programs that can come from different sources. This implies that the analogy has to be carefully studied.

2 BASIC PRINCIPLES

2.1 Systemic-Holistic Approach

The Systemic-holistic Approach, SHA, was developed by [2] for analyzing and studying security problems. It is based on General systems theory, General Living Systems Theory and Cybernetics. General Systems theory was developed by biologist Ludwig von Bertalanffy in 1956 [17, 2]. He

understood the need for having a common research theory for guiding researchers in multi disciplines. The General Systems movement identified laws and principles applicable to various disciplines and which could be used for systems in general. General Living Systems Theory was developed by James Miller [16, 8]. Living systems are in seven categories [16, 2]: they can exist as a cell, as an organ, as an organism, as a group, as an organization, as a nation and as supranational (as European Union). According to Miller the chain of complexity can be built on 19 generic critical subsystems. Out of these 19 subsystems [16, 8], eight deal with processing matter/energy, nine deal with processing information and two subsystems deal with processing both matter-energy and information. This theory helps researchers to link reality and theories. Cybernetics was first defined by a mathematician Wiener [18, 10] as a science of communication and control in animals and machines.

The Systemic-Holistic model is composed of two components: a systemic module and a three dimensional framework [2]. The dimensions in the framework include the levels of abstraction, the context orientation and the content area [2]. The dimension of the levels of abstraction consists of: design or research; theory or model; and physical construction. The context orientation dimension can be geographical space and time bound. The content dimension has the following components: technical issues and non-technical issues. Technical issues include processing, storing, communication, collecting and displaying information. Non-technical issues include operational, managerial, legal, ethical, social and cultural. The Systemic-Holistic approach is used for analyzing and studying security problems, for governing design, operation, management and evaluation of secure systems. This approach can be used to study a system as a whole and the environment of the system and in three dimensions. Different aspects of the security system can be defined, investigated, evaluated and analyzed at any design, theoretical or construction level, and in any time dimension: near future or distant future; and in any environment.

2.2 The Human's Immune System

The human's immune system, IM, is protecting the body from various bacteria and viruses. Most of the information in this section comes from [3, 1, and 4]. The Immune system consists of two main layers: the passive and adaptive layers. The passive layers consist of the skin, membranes, pH (potential Hydrogen of a liquid), temperature and inflammatory responses. The adaptive layers consist of cell mechanisms. All the organisms belonging to a human body are labeled as 'self'. Those organisms that are identified as 'non-self' are detected and destroyed by the immune system. The adaptive immune system reacts dynamically to foreign cells. There are two types of cells that are used in detecting foreign cells: B-cells and T-cells. B-cells are generated in the Bone marrow while T-cells are generated in a Thymus. T-cells are in turn classified as helper T-cells and killer T-cells. Helper T-cells help the B-cells detect foreign cells hidden inside the human cells. Killer T-cells kill foreign cells. B-cells recognize foreign cells and create antibodies with the function to be attached to these foreign cells. Before B-cells are released from the bone marrow they have to be tested whether they can detect correctly. They pass a stage called negative selection in which all B-cells that detect the 'self' labeled organisms are disqualified and deleted. Those B-cells that pass the test are released into the body. When a foreign cell is detected, separate memory cells are created by detecting B-cells to remember the detected foreign cell. Memory cells store information about foreign cells that were detected in the past and these memory cells have longer life spans than normal B- and T-cells. T-cells are also tested using negative selection before being released from the Thymus. Different B-cells and T-cells detect different types of foreign cells. T-cells and B-cells undergo a process called mutation in the gene library. The gene library contains all the genes that are used to create different types of cells. The gene library continuously adapts and creates blue-prints for making better antibodies that detect more and more varieties of foreign cells. The gene library evolves in a process called clonal selection. Those cells that have a higher detecting capacity

are cloned. The genes are used to maintain diversity of antibodies by generating different gene expressions.

The human immune properties have the following features that can be applied in designing better security systems:

- **Distributed** – cells detect the presence of infections locally without any coordination (this can be modeled by having mobile agents act as cells).
- **Multi-layered** – multiple layers are combined to provide overall immunity. (This is already applied in the security architectures).
- **Diversity** – with diversity, vulnerabilities in one system are less likely to be widespread. (This can be achieved by having agents doing a variety of actions).
- **Disposability** – no single system is the most important and any cell can be disposed. Cell death is balanced by cell production. (The technology is not yet ready to implement this feature but at the process / agent level it is possible to implement this).
- **Autonomy** – the immune system does not require outside maintenance or management. It autonomously classifies and eliminates foreign cells and it repairs itself by replacing damaged cells (This behavior is suitable but its implementation is challenging as technology still isn't ready, though it could be modeled so that three or five agents vote for a decision).
- **Adaptability** – the immune system is able to detect and to learn to detect new foreign cells and retains the ability to recognize previously seen foreign cells through immune memory. This feature is not new it in computer systems, though determining that a certain program is malicious with 100% is a hard problem.
- **No secure layer** – no layer is considered more secure than the other.
- **Dynamically changing coverage** - The immune system cannot produce a large enough set of detectors at any moment, so it maintains a random sample of its detectors that circulates throughout the body. This is because there are approximately 10^{16} foreign cells and these have to be distinguished from approx. 10^5 'self'-cells.
- **Identity via behavior** – identity is also proved through the presentation of a behavior (similar to intrusion detection).

2.3 Digital Immune System

Digital immune systems based on the human immune system have been developed. One of these systems has been developed by Symantec [7]. It is used in anti virus systems. The system has a virus detection system, an administrator system, a gateway and a virus analysis center. When a virus is detected on the client side it is sent to the analysis center through the administrator system and the gateway. The administrator system keeps the latest definition files of viruses. It also monitors the samples and results of analysis to and from the analysis center. The administrator system also updates clients' anti-virus programs. The gateway is responsible for securing the network between the client and the analysis center. It controls the network to make sure that the network is not flooded. It is also making sure that only one copy of every sample is sent to the analysis center. When samples of viruses arrive at the analysis center they are put into different classes depending on the languages, file types, versions of viruses and behaviors. The supervisor at the center allocates samples to different machines and human analyzers. The results of the analysis are used to create definition files for different operating systems and for different versions. The definition files are then tested to see if they detect viruses, disinfect files and verify signatures and so on. In some cases the results are not enough to create definition files because the technology of detection is not available for that type of files. This digital immune system is however not effective in detecting polymorphic viruses and power point viruses.

2.4 Generation of Software Agents

In this work we are using software agents to perform different tasks during deterrence, protection, detection and other actions. According to [22], "*An agent is an encapsulated computer system situated in some environment and capable of reactive, pro-active, and autonomous action in that environment in order to meet its design objective*". An agent consists of three main components [23]: header, code, and a database. The header contains identity of the agent, agent attributes, signatures, travel paths, level of trust, ownership and other related information. The code section contains a system of programs performing the specific tasks of the agent. The database contains internal and the collected data while traversing in different environments. Agents are generated from an agent platform like Java Agent Development Framework (JADE) [24]. An agent has to be tested to see if it detects correct. There a number of algorithms for testing and cloning agents of the digital immune systems, but in this work we discuss only two algorithms.

2.4.1 Negative Selection Algorithm

In the first stage of this algorithm normal behavior of programs, users and processes of the system is defined. In the second phase patterns of this normal behavior are created. In the third phase detector agents are created. These agents are then released to monitor the normal programs, users, network traffic or processes. Those agents that detect the normal behavior patterns are deleted, because they are supposed to detect only abnormal patterns. Those detector agents that don't detect the normal patterns are kept.

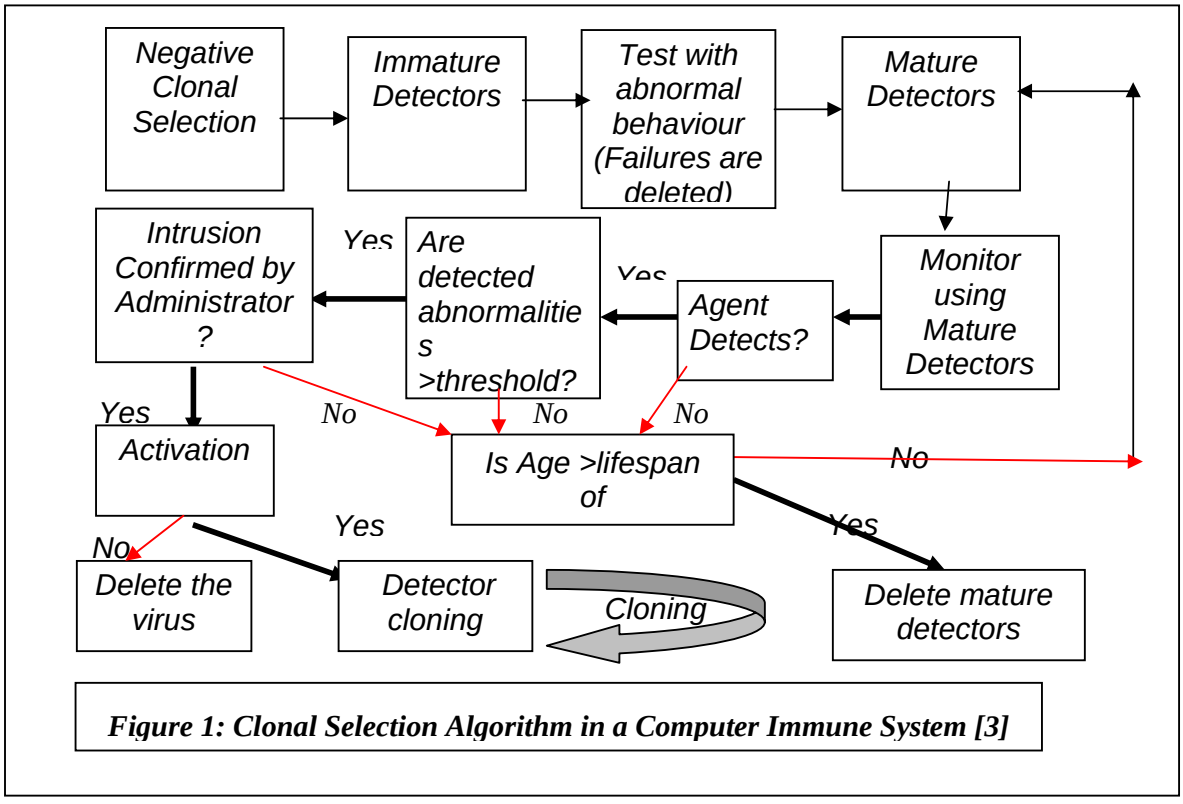

Figure 1: Clonal Selection Algorithm in a Computer Immune System [3]

2.4.2 Clonal Selection Algorithm

This algorithm [3] is shown in figure 1. The immature agents that passed the test during the negative selection algorithm are tested using abnormal behavior. Those agents that pass the test are considered mature and they are released to monitor in real environments. These agents are also monitored to check whether they detect anything. Those agents that don't detect anything are

deleted. Those agents that detect abnormal behavior are kept. In every agent there is a parameter for counting the number of detections, age of the agent and also the type of detections. When the number of detections is less than a specified threshold, the age of the agent is checked. If the age is more than a specified life span the agent is deleted. If the age is not more that the life span, then the agent will continue to monitor. When the number of detections is more than a specified threshold and if a human security officer acknowledges that the detected are foreign cells, the agent is cloned and the abnormality is deleted.

3 METHODOLOGY OF SECURING A SYSTEM

3.1 System model

According to the Systemic-holistic, a system can be viewed and analyzed at the model, design and implementation levels. In this section we analyze the model of the system. The design of the generic security framework will be described in the methodology of securing a system section. The model is based on the systemic-holistic approach and the human's immune system. From the Systemic-holistic approach we apply the features: analysis of the technical and non-technical aspects; analysis of the environment in which the system will be operating; generic view and time factors. The technical aspects include: how to securely store, process, transmit, collect and display information. In this regard we consider technology, software and engineering issues. We check whether the current technology is ready to securely store, process, transmit, collect and display information. Software is concerned with the analysis of security services in the system. It is also concerned with the interfaces, the speed of the operations.

Non-technical aspects include operational, managerial, legal, ethical, social and cultural, people, and information. An analysis has to be made to check whether the system can be accepted by people. Systems interact with people and it is not easy to separate people from operational procedures, managerial, cultural, ethical, social, legal issues. There are different laws in different countries. In some countries a signature can be accepted as evidence in a court only if it is qualified. This means that one can prove the identity of the signer and prove that only he/she signed. The law requires that the keys involve in signing be stored in safe tokens like smart cards. While in other countries it is sufficient to prove that there was an intention to sign some information.

Information can exist in different forms: as protected or unprotected signals: as unprocessed and protected or unprocessed-unprotected message: as processed and protected or processed and unprotected message: as protected or unprotected knowledge. Knowledge refers to information that has some meaning to the reader. Information can be further classified as being ethical, legal, according to the security policy, as politically correct, in accordance to a specified culture. Information could be further classified into sensitivity levels (green, orange, red, etc), quality of service required (high, medium, low; emergency, etc). As [13] points out ethical, laws, policy, standard operation procedure headers can be added to information and messages have to be approved before being sent to other parties.

Considerations have to be made regarding time, environment, political and security policies. With time technology changes and so considerations have to be made about how future can affect the system. Room has to be given for extensions of the system. According to [20] "*The observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months*". This law has so far proved to be working even though the software is not developing at the same speed as hardware. It is possible to design many transistors theoretically, but it completely another issue to have that

many transistors in one chip. Another example is that PC manufacturers are aware that PCs have to interact with TV sets, stereos, mobile and non-mobile phones and other home and office appliances. If these factors were considered by PC manufacturers from the beginning the current PCs would be accommodating these features and the prices of the PCs would have been relatively low. But manufactures have to redesign PCs to meet the new requirements. In the near future the PCs will be acting as databases for storing stream videos, pictures, music and other media. These media will have to be transferred to TVs and stereos. This can be done using wires or without wires and so the PCs have to be equipped with the capability of doing this. These examples and Moore's law show that we can predict future applications in today's system designs.

From the Immune system the following features are applied in the model: Adaptability; autonomy; multiple layers, identification; memory; diversity; distribution; dynamic coverage as shown in figure 2. The features in this model, figure 2, that are based on SHA and IM are combined to form a system with five main sub-systems: deterrence, protection, detection, response, and recovery.

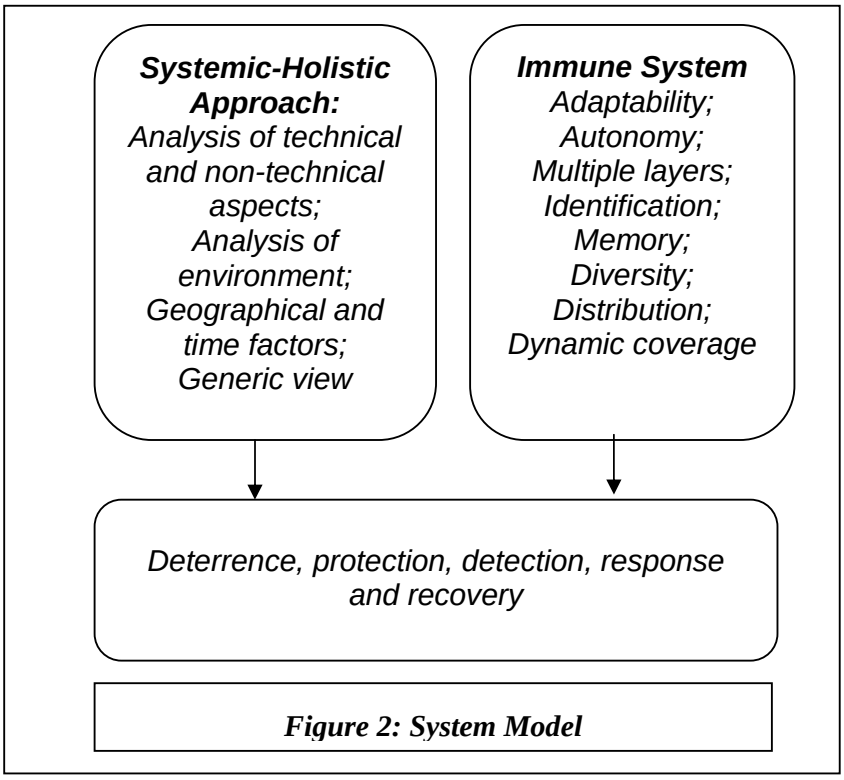

Figure 2: System Model

3.1.1 Deterrence Sub-System

Deterrence sub-system is aimed at scaring off attackers (like how a cat scares off attackers by increasing its size and through fierce screams). When criminals plan to rob a bank in the physical world they do surveillance of the bank to determine whether it is possible to attack, take what they want and get out without being caught and without living evidence. In the digital world the attackers do more or less the same. Before would be attackers intrude a system, they do some kind of scanning to determine the operating systems and their versions, the ports that are open, the applications and versions that and on the victim's system. Then the attackers do possibly also social engineering to understand the architecture of the system inside. There are many ways of doing this, from just asking the people working there to listening to conversations of system administrators

there or secretaries working there. It is surprising how employees like to talk about their jobs during lunches and even dinners! From the results of scanning and social engineering the criminals decide whether it is possible to attack the system, and get out without being caught and without living evidence. The attackers will not attack a system if it is considered to risky. So there has to be means of scaring the would-be attackers from attacking a system. The functions of the deterrence sub-system include: adapting to the new and unknown surveillance methods; organizing training to prevent social engineering; monitoring surveillance attempts; redirecting attacks to specialized environments (like honey pot system); handling replies to scanners (returning nothing, a warning, etc); auditing; tracing scanning sources.

3.1.2 Protection Sub-System

Protection is a sub-system for guiding the territory of a system and its entities. Home cats establish territories, a special place on a sofa, and put rules. Wild cats mark territories by using peculiar identifying items like natural scents. The protection sub-system provides the following security services: authentication, integrity, confidentiality, non-repudiation and authorization of entities and information during storage, transmission, processing, collection and display. Other features of this sub-system include: adaptability in which the system learns new protection ways by applying the latest standards; organizational, like configurations in accordance to the security policy; semi-autonomy in which the system makes some decisions without involving the management of the system, but the critical decisions must involve the system management; multi-layer protection , where protection is provided at the boundary of a system and inside the system and sub-systems; partial distribution – in some cases protection is done locally while in some cases protection is coordinated. Software agents will be used to provide most of these features as described in section 3.2.

3.1.3 Detection Sub-System

This sub-system is responsible for detecting the abnormalities, storing and protecting the log of events, analyzing the events, monitoring, management and interacting with other subsystems. Other features include multiple-layer detection, adaptability of new ways of monitoring and detecting, semi-autonomous, and dynamic coverage, sending reports to the database and the administration. The normal behaviors of outgoing and incoming messages are defined. Software agents are used to detect the abnormal behaviors of incoming and outgoing messages, as cells are used to detect foreign cells in immune systems. All the entities that belong to a system are labeled as ‘self’ by being given special identities and being registered in a database. Software agents monitor a system to discover the non-self entities in a system.

3.1.4 Response Sub-system

This sub-system is responsible for incident management. It classifies incidents into false alarms, minor and major incidents in accordance with the security policy of the system. The response and speed of reaction depends on the classification. It makes decisions on how to respond for every incident. The decisions include disconnecting the affected sub-system from others, slowing, shutting down or restarting the affected system, etc. The sub-system also sends reports to the affected users, to the database and to the administration. Other functions of this sub-system include managing patches and adaptability, tracing the attack, mitigation of the attack and so on.

3.1.5 Recovery Sub-System

The recovery sub-system is for bringing an attacked system back to normal. The functions of this sub-system include managing back-ups, re-installing the programs, periodic and emergency vulnerability testing, restoring a system from back-ups, collecting and protecting evidence, fixing the vulnerabilities. The agents can help to define and test business continuity plans. This process

can be very expensive and takes much time if done manually. At every moment three types of the state of system and sub-systems and operations are stored: the original state; the intended state; and the actual state. When an incident occurs the system can go back to the original state and flush all the rest. This feature can be partially or wholly implemented depending on the current technology and other back-up resources.

3.2 Generic Security Framework

The generic security framework is composed of five main sub-systems: Deterrence, protection, detection, response and recovery as shown in figure 3. Every sub-system can be implemented using human, hardware or software [13] or combined, depending on: the decisions that have to be made; the time of decision; and also the sensitivity of the environment like whether it is for a nuclear plant, a military, a bank and so on. How much effort should be spent [13] on deterring, protecting, detecting, responding, recovering and the interaction with people depends on the environment. One telecommunications company uses 0% in deterrence; 70% in protection; 5% in detection; 5% in response; 20% in recovery in form of insurance fees. The dictatorship governments use approximately 80% of the resources in deterrence; the rest 20% is used for protection, detection and response. This should be specified in a policy file. One example could be to put 10 % of the effort on deterrence, 50 % on protecting, 20% on detecting, 10% on response, 10% on recovering.

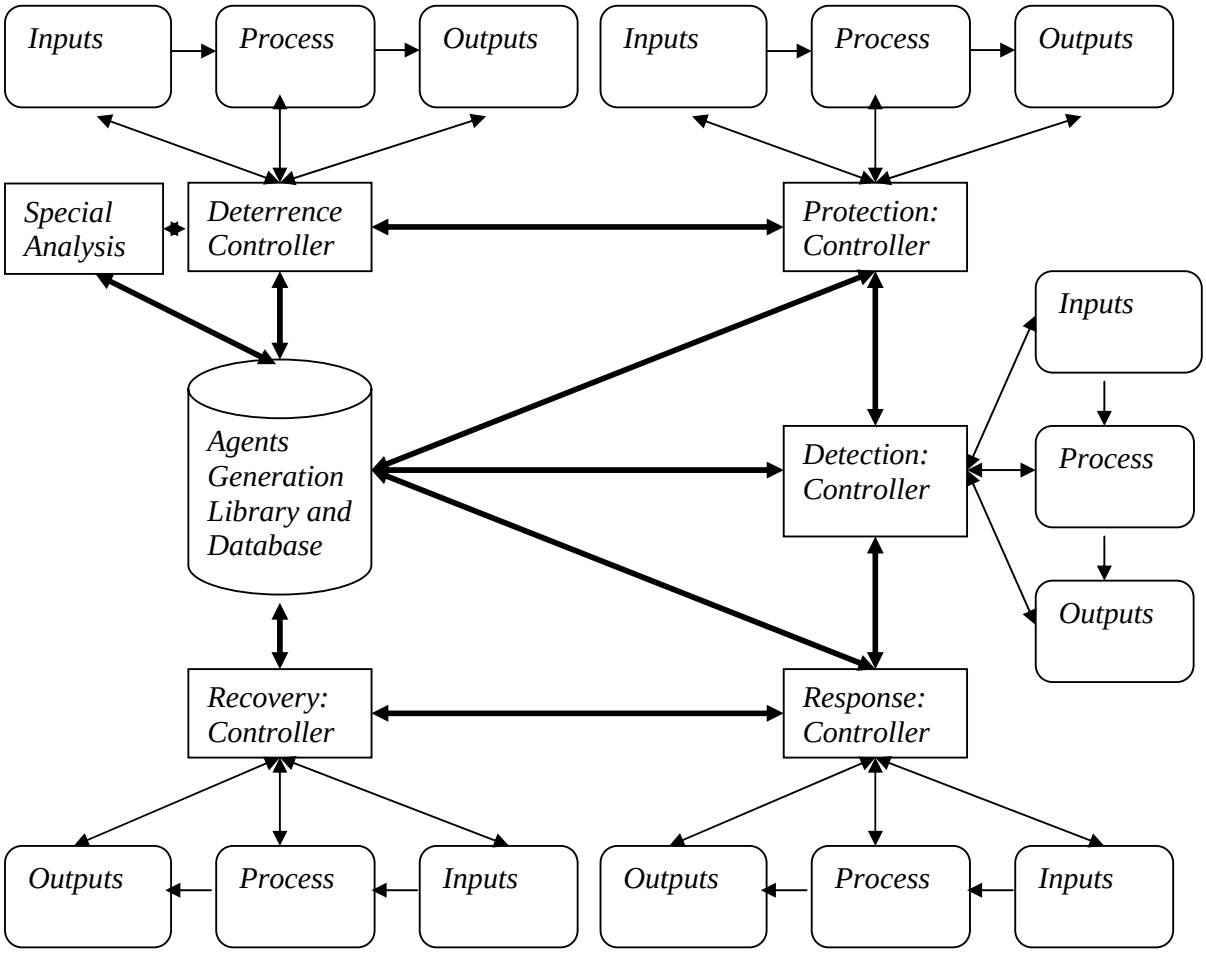

Figure 3: Generic Security Framework

The Immune system uses cells to detect viruses. This framework uses software agents to perform different specialized tasks. The agents are generated in the agent generation library using an agent platform like [24]. Every sub-system requests the agents it needs from this library. Agents are tested and sent to the requesting sub-system by using negative selective and cloning algorithms like those described in [3]. All the sub-systems have a controller, an inputs section, a processing section and an outputs section. The deterrence controller interacts with the inputs, process and outputs sections. It also communicates with the protection sub-system and the agents' generation library and database. When surveillance attempts come to a system they pass through the deterrence controller. The controller analyzes them and sends them as inputs to the process or to the special analyzer for further analysis. The controller also sends these incoming surveillance attempts to the database. Before being sent to the database and to the special analyzer the incoming surveillance attempts are encapsulated. All the other sub-systems have feedback mechanisms with the aim to learn and improve the processing. All the sub-systems interact with the agent generating library and with each other to share the knowledge needed to learn and improve processing.

There are three types of feedback mechanisms [18]: first order; second-order; and third-order. The first-order mechanism does not improve a process. The second-order has a memory and can help in improving a process but it has a limited number of unchangeable feedback alternatives making it less dynamic. Third-order has memory, many feedback alternatives and is more dynamic than the other alternatives. In this framework we aim for the third-order feedback mechanism. The controller combines different inputs; modifies inputs; stores different types of inputs; and manages different operations for improving processing in every sub-system. For every stage the processing can have a number of sub-processes like decision making, searching, memory unit, selecting, re-combining different factors [2], etc.

Every sub-system has generic functions which can be replaced or updated whenever necessary. The security level of every system is based on three types of factors: users of the system; the system policy; and the policy of the environment in which the system is located. This generic security system sets a minimum level of security for all systems regardless of the environment the system is running in. This level can be increased depending on the type of environment, the type of users and the system policy.

3.3 Limitation of the System

The framework has not been implemented and so there are no results of performance yet. Some aspects of this framework may not be wholly implemented by today's technology and it is highlighted as a challenge to the researchers to come up with the technology for implementing them.

4 CONCLUSION

The generic security framework provides a methodology for securing systems. It is based on Systemic-holistic approach and the Immune system. Security is not only about technology but it about people using the technology and the environments in which the systems are operating. This paper has suggested a methodology of generically viewing security systems. Future work will include implementing the framework, which we have just started working on. Future work will also include developing more effective algorithms for the agents.

5 REFERENCES

[1] A. Somayaji, S. Hofmeyr and S. Forrest. Principles of Computer Immune System, 1997 *New Security Paradigms Workshop, ACM p75-82*

[2] Louise Yngström. A systemic-Holistic Approach to academic programs in IT Security, Ph. D thesis, Stockholm University / Royal Inst. of Technology ISRN SU-KTH/DSV/R--96/21--SE, 1996.

[3] Jung Won Kim, Integrating artificial Immune Algorithms for Intrusion Detection, Ph. D thesis, University of London, 2002

[4] Anastasios Grigoriadis, Requirements for computer immune defense System based on body's immune System and DNA proofing. Masters thesis: Stockholm University, 2003.

[5] J. H. P. Eloff and S.H. von Solms, Information Security – the next Decade, IFIP 1995, ISBN 0-412-64020-1

[6] Matt Bishop. Computer Security Art and Science, Addison-Wesley 2003, ISBN 0-201-44099-7

[7] Carey Nachenberg. Understanding and Managing Polymorphic Viruses. *Symantec Press papers*. www.Symantec.com, 2004.

[8] B.S. Coffman, James Miller's Living Systems Model. http://www.mgtaylor.com/mgtaylor/jotm/winter97/millerls.htm, 2004.

[9] Symantec, Digital Immune System, www.symantec.com, 2004

[10] Web Dictionary of Cybernetics and Systems, www.pespmc1.vub.ac.be/ASC/indexASC.html, 2004

[11] Arne Kjellman. Constructive Systems Science – the only remaining alternative? Ph. D thesis: Royal institute of Technology. 2003. ISRN SU-KTH/DSV/R—03/14--SE

[12] Jeffy Mwakalinga, Security Management of Global and Integrated Security System, ISRN SU/KTH/DSV/R—02/30—SE

[13] Stewart Kowalski, IT Insecurity: A Multi-disciplinary Inquiry. Doctoral thesis: Royal Institute of Technology. 1994. ISBN: 91-7153-207-2

[14] Hofmeyr, S., The Implications of Immunology for Secure Systems Design in Computers and Security. 2004 Chapter 23, 454 – 455.

[15] Schoederbek, P., Schoederbek, G., Kefalas, A., Management Systems. Conceptual Considerations: 4th ed., Irwin Boston, 1990

[16] Miller, James, G., Living Systems, McGraw Hill, 1978

[17] von Bertalanffy, L., Main Currents in Modern Thoughts, in Yearbook of the Society for General Systems Research, Vol 1, 1956.

[18] Wiener, N., Cybernetics and Control of Communication in the Animal and Machine, John Wiley and Sons, 1948.

[19] http://uhaweb.hartford.edu/BUGL/

[20] http://www.webopedia.com/TERM/M/Moores_Law.html (22-04-2005).

[21] Mwakalinga, J., Muftic, S., Risannen, E. Authorization System in Open Networks Based on Attribute Certificates, 5th IITC2004 Proceedings.

[22] N.R. Jennings. Agent-Based Computing: Promise and Perils. Proceedings of the Sixteenth International Joint Conference on Artificial Intelligence. Stockholm, Sweden. Pp.1429-1436, 1999.

[23] Y. Cheng. A comprehensive Security Infrastructure for Mobile Agents. ISRN SU-KTH/DSV/R—97/13—SE. 1997

[24] F. Bellifemine, T. Trucco. Java Agent Development Framework: http://jade.tilab.com/index.html. (15-04-2005).

6 PERMISSIONS