BASIS: A Biological Approach to System Information Security

Victor A. Skormin[1], Jose G. Delgado-Frias[2], Dennis L. McGee[1], Joseph V. Giordano[3], Leonard J. Popyack[3], Vladimir I. Gorodetski[4] and Alexander O. Tarakanov[4]

[1]Binghamton University, Binghamton NY, USA
[2]University of Virginia, Charlottesville VA, USA
[3]Air Force Research Laboratory at Rome NY, USA
[4]Russian Academy of Sciences, St. Petersburg, Russia

1. INTRODUCTION

With the increase of size, interconnectivity, and number of points of access, computer networks have become vulnerable to various forms of information attacks, especially to new, sophisticated ones. It should be pointed out that biological organisms are also complex and interconnected systems that have many points of access; these systems are vulnerable to sabotage by alien microorganisms. During evolution, biological organisms have developed very successful immune systems for detecting, identifying, and destroying most alien intruders. In this paper we intend to establish a connection between the basic principles that govern the immune system and potential uses of these principles in the implementation of information security systems (ISS) for computer networks. In order to be dependable, existing ISS require an enormous amount of data processing that adversely affects the network performance. A modern ISS must include a number of semi-autonomous software agents designated to prevent particular kinds of threats and suppress specific types of attacks. The ability of such an ISS to provide the required level of information security without burdening the network resources could be achieved only by adopting the most advanced principles of interaction between particular agents. Such principles have been used in biological immune systems. These systems have distributed cells (agents) of various types that attack anything suspected to be alien. Cells interact by sharing information about the type and location of an intruder, utilize the feedback principle for engaging only "as many cells as necessary," and are capable of learning about intruders that results in immunity to repeated attacks.

When necessary functions of the ISS agents are established, the multi-agent system theory can be utilized as a mathematical apparatus to facilitate the formalization of the complex interaction between particular agents in the fashion that is observed in biological immune systems. The individual and collective behavior of particular immune cells need to be investigated to establish a synthetic immune system operating in computer networks.

1.1 The Problem of Information Security

The problem of information security has been recognized as one of the most complex and its importance is growing coherently with increasing network connectivity, size, and implementation of new information technologies. Today, information has become a highly valuable commodity and its vulnerability is of great concern within any large-scale organization utilizing computer networks. Networks and information are becoming increasingly vulnerable to intrusion due to newly developed direct and remote threats and attacks. According to a widely accepted point of view *intrusion* is defined as "any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource" [1]. According to this definition, there exist three *major types of threats for information security* [2, 3, 4, 5, 8, 9, 10]:

1. threat of *non-authorized access* to information,
2. threat of *destroying information integrity*, and
3. threat of *denial of service* making crucial resource and/or information unavailable.

Current computer security systems consist of a number of independent components requiring an enormous amount of distributed and specialized knowledge to solve their own security sub-problems. As a rule, these systems represent a bottleneck with regard to process speed, reliability, flexibility and modularity [6].

This paper has been organized as follows. In Section 2 a brief outline of the approach is provided. Some basic principles of a biological immune system are described in detail in Section 3. The major components of the proposed Biological Approach to System Information Security (BASIS) are presented in Section 4. Some concluding remarks have been drawn and presented in Section 5.

2. PROPOSED APPROACH OUTLINE

BASIS, proposed in this paper, reflects the similarities between the computer network security problem and the task of protecting a biological system from invading microorganisms. We propose to synthesize an ISS of a computer network that follows the basic principles of operation of the biological immune system. The utilization of biological defensive mechanisms developed by evolution has a great potential for the assurance of information security in large-scale computer networks.

With the complexity of modern information security systems, an ISS must be considered as a number of independent, largely autonomous, network-based, specialized software agents operating in a coordinated and cooperative fashion designated to prevent particular kinds of threats and suppressing specific types of attacks. This approach provides the required level of general security of information according to a global criterion. A biological immune system of an advanced organism already has been considered as a good and clear example of a modern agent-based ISS [7, 13]. The *immune system* consists of distributed white blood cells, which attack anything that they consider alien. By having as many cells as necessary, the animal body is able to defend itself in a very efficient way. If the animal body is infected in one area, then cells move to that area and defend it. Modern multi-agent system technology presents a valuable approach for the development of an ISS that is expected to have very promising advantages when implemented in a distributed large scale multi-purpose information system. An agent-based model of an ISS, consistent with the BASIS concept, is described in [11].

Our ISS approach can be viewed as a set of semi-autonomous distributed agents capable of detecting, recognizing, pursuing, and learning about the attackers. The algorithms of agents' individual behavior need be consistent with those established in immunology. While the implementation of particular ISS agents may be computationally intensive, a feasible ISS system requires a high degree of interaction, coordination, and cooperation between agents. It is believed that these, almost intelligent, interactions constitute the centerpiece of a biological defensive mechanism and assure its high efficiency. Until recently, quantitative description of the cooperative behavior of semi-autonomous agents presented a problem that could not be solved within a general framework. Such a framework has been provided by the multi-agent system approach. This framework facilitates the development of the rules and procedures of the interaction between ISS agents thus leading to the development of a feasible ISS operating as an artificial immune system. The feasibility of such an ISS could be assured only by the implementation of the rules of agents' collective behavior observed in a biological immune system that could be formalized using the multi-agent system theory.

Research in immunology has established various mechanisms of individual behavior of cells resulting in their ability to detect, identify, pursue and destroy an alien entity; to accumulate knowledge on attackers, to adopt behavior to a new situation; and to determine the proper response. These mechanisms, developed by evolution, are highly efficient and successful. In addition to individual cell operation, immunology presents numerous examples of collective, almost intelligent, "unselfish" behavior of various types of defensive cells. This collective cell behavior allows the achievement of high efficiency and minimum response time of the immune system, as well as maximum utilization of its limited resources. The major difference in the targets between the immune system and an ISS is: the immune system treats as an "enemy" *any foreign entity* within the organism, while an ISS must recognize and treat as an "enemy" *any illegitimate entry* or *software*. Table 1 shows some of the similarities between the two systems.

A number of mathematical models of individual behavior of defensive cells utilizing methods of statistics, discrete mathematics, and numerical simulation, have been successfully implemented. The attempts to develop an artificial immune system that could be applied for such a practical problem as information security assurance are much less successful, primarily because of the necessity to describe mathematically cooperative cell behavior. However, modern multi-agent system technology presents the most plausible approach for solving this problem in the framework of the development of an ISS. The resultant ISS would operate as a synthetic immune system and is expected to have very promising advantages when implemented in a distributed large-scale multi-purpose computer information network.

We propose the following steps to achieve ISS by means of biologically inspired schemes:

a) *Analysis and Qualitative Description of Immune Systems.* An analysis of the recent biological research and development of a comprehensive qualitative description of the operation of a biological immune system are needed to capture the behavior immune system as it may relate to ISS-related problems.
b) *Algorithmic Description Immune Cells.* The next step is to develop a mathematical/algorithmic description of the individual behavior of immune cells utilizing already established methods and models, and their cooperative operation using the multi-agent system theory.
c) *Software Implementation of Models.* A software implementation of the established mathematical models, rules and algorithms resulting in an ISS operating as an artificial immune system is necessary to test and check these models.
d) *Simulation Environment.* A simulation environment suitable for the representation of a computer network with a resident ISS and various forms of threats and attacks needs be developed to prove the model.

e) *System Analysis.* Simulations need to be analyzed to fine-tuning of the resultant ISS, This analysis should include assessment of its impact on the network vulnerability.

The BASIS approach requires a multidisciplinary effort; the disciplines included are: advanced control theory, mathematics, computer science, computer engineering, biology, information warfare, and computer programming.

Table 1. Similarities Between Biological and Computer Systems

Biological Systems	**Computer Networks**
High complexity, high connectivity, extensive interaction between components, numerous entry points.	*High complexity, high connectivity, extensive interaction between components, numerous entry points.*
Vulnerability to intentionally or unintentionally introduced alien microorganisms that can quickly contaminate the system resulting in its performance degradation and collapse.	*Vulnerability to malicious codes (including computer viruses) that being introduced in the system result in unauthorized access to information and services and/or denial of service.*
Alien microorganisms as well as cells of a biological system are composed of the same building blocks - basic amino acids.	*Malicious codes as well as the operational software of a computer network are composed of the same building blocks - basic macro commands.*
The difference between alien microorganisms and the healthy cells of a biological system is in the (gene) sequencing of their building blocks.	*The difference between malicious codes and the operational software of a computer network is in the sequencing of their building blocks.*
Biological immune systems ***are capable of*** *detecting, recognizing and neutralizing most alien microorganisms in a biological system.*	*Information security systems* ***should be capable of*** *detecting, recognizing and neutralizing most attacks on a computer network.*

The immune system, like computer network systems, is extremely complex. It comprises a massive whole body response mechanism involving multiple cell types and specialized tissues. For the purpose of feasibility, the immune system needs to be represented/modeled in its basic components and then one could consider the interaction of these components resulting in a complete body response to three generalized foreign agents: a toxin, a bacteria, and a virus. The toxin represents a foreign agent presented to the system in large amounts (e.g. injected or swallowed) or produced in large amounts by an infectious agent which causes harm to the host system. In a computer network environment, effects of a toxin could be paralleled with an illegal entry which results in the destruction of significant amounts of resident data. The bacteria would be an agent which can replicate itself independent of the host and which causes harm to the host system. A corresponding attack on a computer network would comprise an illegal entry facilitating future illegal utilization of the network facilities including the ability to manipulate confidential information. Finally, the virus would represent an agent which replicates itself through the host system and which then would cause harm to the host. Unsurprisingly, growing and replicating itself using the host facilities at the expense of resident software, is exactly what a computer virus does rendering the network useless.

3. INFORMATION SECURITY TASKS IN A BIOLOGICAL IMMUNE

A detailed description of the biological immune system is provided in this section. This description includes the basic immune system response, the major players in this system, and the interaction of these components.

3.1 The basic immune response

A basic immune response can consist of one or more of three components [1], [2]. The first component is the innate or non-specific immune response. It consists of anatomic or physiological barriers (e.g. the skin and the acidity of the stomach) and the inflammatory response that is responsible for the redness and swelling at a wound site and the influx of cells such as neutrophils and macrophages which phagocytize. This innate immune response does not show specificity for any particular foreign agent and does not show an enhanced response, or

memory, with the second encounter. For all practical purposes, the innate immune response could be paralleled with a system of passwords, intended to prevent unauthorized access to the network. This can be considered as the "skin" of a computer system. Its response is prompted by reading a password -an "external label" that has nothing to do with the internal nature of the attacker. At the computer network level, innate responses could include firewalls that do not allow intruders to get into a sub-network. In this case the ID domain would prevent any other user from a different domain (non-self) to get access to any computer in the present domain (self).

The other two responses show specific acquired or adaptive immune responses. These responses show the exquisite capacity to specifically recognize unique foreign substances (or antigens as they are called), distinguish self from non-self, and show a heightened and rapid memory response with each subsequent encounter with the antigen. The humeral immune response has classically been defined as a response of the body to foreign antigens by producing large amounts of antibodies; serum proteins which have a binding site that binds with high specificity to the antigen (or a defined portion of the antigen) to inactivate the antigen or allow for the removal of the antigen. The B lymphocytes cells (or B cells) produce these antibodies. Antibodies generally work only on antigens which are found exposed in the body such as floating in the blood or body fluids (e.g. toxins) or on bacteria, viruses, etc. which are exposed and not sequestered inside of an infected cell. These antibodies are useful in clearing the infectious agents or toxins from the body fluids and tissues. The computer equivalent of this response is the ability to distinguish between a legitimate user and an illegal intruder that successfully penetrated the system. In general, messages/programs containing system calls are considered suspicious [12]; thus the internal composition of these messages/programs can be used to determine self and non-self. Non-self messages/programs need be discarded by specialized software (antibody) that deals with this type of attackers. This response is facilitated by the ability to recognize an attacker because of its foreign internal nature as well as behavior.

The cell-mediated immune system has evolved to attack extracellular bacteria and viruses along with those infectious agents which may be hidden inside of cells. These infected cells become factories that produce the viruses or bacteria, yet in many instances the antibodies cannot get to the infectious agents sequestered inside of the cell -therefore, the infection persists. This cell-mediated immune system then uses either specialized killer cells (cytotoxic T lymphocytes or CTLs, see below) with highly specific cell surface receptors to recognize and kill virus infected cells or other antigen-specific T lymphocytes (T_{DTH} cells) to direct the action of non-specific types of cells such as the phagocytic macrophages to destroy bacteria, protozoa or fungi. The computer equivalent of this response is based on the ability to detect a hidden attacker disguised as or within a legitimate piece of software. For instance, an email may contain a malicious virus; this virus is hidden within an apparently legitimate piece of software. Antivirus programs are usually utilized to deal with these problems. However, these viruses need be recognized by a immune-like system before these cause any major harm.

Of importance to note, the mechanisms which regulate the activation and function of these immune cells are very stringent and complex. Without proper regulation, the immune system would over-respond to foreign agents resulting in potential harm to the host or the system may allow self reactive cells to function resulting in deadly autoimmune responses. By its nature, this effect is nothing but a sophisticated feedback mechanism that could be implemented in a computer network. Table 2 presents a summary of the immune system responses along with some parallel responses of computer/network systems.

Table 2. Immune and computer system responses

Immune Response	Immune System	Computer/Network System
Innate or non-specific	Anatomic or physiological barriers (e.g. the skin and the acidity of the stomach) and the inflammatory response.	System's passwords and firewalls that do not allow an intruder to get into a closed sub-network.
Humeral	Antibodies identify antigens and help to clear the body from infectious agents.	Specialized software help to identify system calls in messages/programs. "Non-self" programs are discarded.
Cell-mediated	CTL and T_{DTH} cells are used to destroy bacteria, protozoa or fungi.	Antivirus programs specialized on a particular computer virus.

3.2 Immune response major players

Antigens may be composed of several types of compounds (protein, sugars, lipids, etc), however protein antigens are the type that induce the most vigorous response. Proteins are comprised of chains of simpler

compounds called amino acids. Since there are 20 different amino acids, the combinations of the amino acids can yield an incredible number of possible distinctly different proteins.

The antibodies are proteins themselves which, by the nature of their amino acids at the binding sites, can bind strongly to specific short sequences of amino acids. These specific amino acid sequences may then appear within the longer sequence of a certain protein and therefore the antibody can "recognize" the protein via this shorter sequence and then bind. One important property of this antigen-antibody recognition system is that it is extremely specific. However, antibodies may also bind, with lesser strength, to amino acid sequences which are almost identical to the recognized sequence allowing for "cross-reactivity" of the antibodies. This could allow the antibodies to recognize a slight variation of the original infectious agent and therefore confer some immunity. Yet the more different the sequence is from the recognized sequence, the greater the chance for non-recognition. Another important consideration of this system is that in general, a specific antibody must exist for essentially all of the antigens which one could possibly encounter. Still, the immune system has the capacity to randomly generate more than 10^{11} different antigen binding antibodies.

The antibody proteins are produced by the B cells. These cells randomly generate the capacity to produce an antibody with a single antigen recognition site such that one B cell produces an antibody which recognizes only one antigen (to have a cell which produces several antibodies which recognize different antigens would be a regulation nightmare!). This B cell then produces the antibody only as a cell surface receptor and remains in a resting state, waiting to encounter the specific antigen. When the antigen is encountered, it binds to the antibody on the B cell surface and stimulates the B cell to awake and get ready to function. However, in most instances, the B cell cannot begin to undergo cell division (to amplify the number of antigen specific cells and therefore amplify the response) or begin secreting antibodies until it obtains a second signal from a Helper T lymphocyte (Th cell). This prevents the B cell from producing potentially harmful antibodies without a confirmation that the response is needed. Once the B cell is activated, it then begins to differentiate into either a Plasma Cell, which produces large amounts of antibodies and then dies, or a Memory Cell which eventually reverts back to a resting state and waits for a second encounter with the antigen. These Memory Cells are the basis of the greatly elevated and rapid memory response to the same antigen, as there are now greater numbers of these cells present which now have a less stringent requirement for activation.

As mentioned above, the B cell requires a second signal from a Th cell in order to continue its activation sequence. This Th cell is also an antigen specific cell with a specialized receptor, called the T cell receptor, for a very specific antigen amino acid sequence. The T cell receptor is similar to the antibody molecule, yet it is limited in its ability to recognize and antigen. During development of the Th cell (indeed all T cells including the CTLs and T_{DTH} described below), the cells pass through a specialized tissue, the thymus, in which cells with T cell receptors that recognize self-antigens are killed. This eliminates the majority of the self reactive cells and does an excellent job of preventing autoimmune responses. Also in the thymus, only the T cells with T cell receptors which can recognize antigen segments which are "presented" to them by accessory cells with specialized cell surface antigen-presentation receptors, the Major Histocompatability Complex class II receptors (MHC II), are allowed to survive. Indeed, it has been estimated that greater than 90% of the T cells in the thymus never survive these stringent regulatory requirements to leave the thymus.

Once a Th cell leaves the thymus, it is fully capable of functioning, yet, like the B cell, it too is in a resting state. The T cell receptors of these Th cells cannot recognize antigens alone so they cannot be activated directly by antigen. In the case of the humoral immune response, the B cell binds the antigen via its cell surface antibody which gives the B cell its first activation signal. This antibody bound antigen is then taken internally by the B cell and "processed" into short amino acid segments which are then "loaded" onto the MHC II receptors. The B cell then places these MHC receptors loaded with antigen segments on its surface and is now ready to interact with a Th cell. This interaction then consists of the B cell "presenting" the antigen to the Th cell to activate the Th cell. This presentation of the antigen-MHC II to the Th cell provides an activation signal for the Th cell to begin cell division (amplification of the response) and to differentiate into a mature helper T cell capable of helping the B cell. The mature, activated Th cell then produces signals (via cell surface receptors or small secreted factors) which tell the B cell to continue on its activation sequence to cell division and antibody secretion.

Of interest, this B cell-Th cell interaction presents another site for amplification of the immune response. One B cell can "process" a large antigen into several small different segments which could be used to activate several Th cells with different antigen specificities. This would increase the probability that the B cell would get a second signal from a Th cell even if the Th cell did not recognize the exact same segment of the antigen amino acid sequence that the B cell recognized. Also, a single activated Th cell could then interact with several B cells to allow the production of several different types of antibodies (one specific type from each different B cell). However, only those B cells which have encountered the antigen for the first activation step would be sensitive to the Th cell help. The overall response would be a more complete activation of several B cells and T cells with different antigen specificities - essentially responding to several different segments of a single antigen.

Before continuing, another important group of cells must be considered. These are the accessory cells which are not antigen specific but play a very important role in the immune response. The accessory cells consist mainly of macrophages and dendritic cells which function to engulf or phagocytize cells, bacteria, viruses, or even cellular debris and proteins. These engulfed cells or substances are then enzymatically destroyed and "processed" much like the B cell processes antigens bound to their cell surface antibody receptors to yield short segments of amino acids. As in the B cells, these antigen segments are also loaded onto MHC II receptors for the accessory cells to "present" to any nearby Th cells. Indeed, the initial activation of most Th cells usually occurs via the presentation of foreign antigens by these accessory cells. This system then allows for the constant sampling of the body's environment via macrophage phagocytosis (for bacteria, viruses, and etc.) or dendritic cells (for cell debris and individual proteins). Therefore, antigen sampling (and hence Th cell activation) is not limited to antigen specific B cells only, but also certain non-specific accessory cells.

In the cell-mediated immune response, one of the most potent killer cells is the CTL, a T cell with a T cell receptor which recognizes foreign antigens present inside of an infected cell. Like the B cell, this CTL is normally in a resting state and needs two independent signals for activation. The first signal comes when the resting CTL encounters an infected cell. Almost all cells of the body have an internal system which constantly destroys old proteins as new ones are produced by the cell. The destruction of old proteins results in the production of short amino acid segments which may then be loaded onto a different type of MHC receptor called the MHC class I receptor (MHC I) which is then placed on the surface of the cell. Therefore, most cells of the body constantly display a variety of "self" amino acid segments in conjunction with the MHC I receptor on the surface of the cell. However, when a cell becomes infected with a virus, the virus uses the cells machinery to replicate itself. Yet this replication of the virus inside of the cell allows the cell's internal system to sample some of the virus proteins by destroying them and placing the short virus amino acid segments onto the MHC I receptors (again, random sampling as with the accessory cells above). Subsequently, when the viral antigen loaded MHC I receptors are on the surface of the cell, the cell is now labeled as an infected cell even though the immune system cannot directly get at the virus inside of the cell.

Once a CTL comes in contact with a virus infected cell, if its T cell receptor can recognize the virus segment, then the CTL obtains its first activation signal. However, the CTL cannot be completely activated until it receives help from a Th cell which has also been activated. The activated Th cell (usually activated by antigens from the same virus as presented by accessory cells) then produces a T cell growth factor (interleukin-2) necessary for the CTL to begin cell division (once again, an amplification step) and mature into a functional CTL. As with the B cells, memory CTLs are also produced to produce a memory response in subsequent encounters with the virus. When the mature CTL encounters the virus infected cell again (via the T cell receptor binding to the virus antigen segment and the MHC I receptor), the CTL kills the virus infected cell. Of importance, the mature CTL can kill many virus infected cells over its life span.

The final player in the cell-mediated immune response is the T_{DTH} cell. Once again, this T cell has an antigen specific T cell receptor and must have the antigen presented by an accessory cell along with MHC II. They are essentially helper T cells which have their first encounter with the antigen in the lymph nodes. They then undergo cell division (amplification of the response) and maturation to competent T_{DTH} cells. These cells then leave the lymph nodes and actively seek out the areas of infection (see below how they are recruited into areas of infection). They migrate into the area where they receive the second encounter with the antigen (presented by resident macrophages actively phagocytizing the bacteria or viruses or dendritic cells sampling the infection debris) and then produce large amounts of inflammation inducing factors or cytokines which activate the phagocytic macrophages, neutrophils and other cells in the area.

3.3 The interaction of the immune system components

The immune system components interact in a particular way or fashion depending on the type of foreign agent that the biological organism is exposed to. In this subsection we describe the immune system respond against toxins, bacteria, viruses, and infections.

3.3.1 Immune system respond against toxins.

In the case of a toxin, the best defense is the antibody molecule. A toxin by itself usually can cause harm to the cells of the body and therefore must be neutralized. This is usually effectively done by the binding of the antibody molecule (usually by blocking the toxin from entering into a cell or blocking the toxin function). Therefore, the major players in the anti-toxin response would be the B cell which produces an antibody to neutralize the toxin and the Th cell which provides help for the B cells. However, macrophages can also have a role in these responses by providing another cell type to present the toxin antigens to Th cells. Macrophages also have receptors on their cell surface which can bind to antibodies which have bound to an antigen (these receptors often do not bind well to antibody which has not bound to an antigen). This then provides a way for

the macrophage to attach to the antigen and engulf or phagocytize the toxin to remove it from the body. Finally, some toxins may also activate macrophages and induce them to secrete soluble factors which can enhance B cell division, antibody production, and Th cell responses. On the second encounter with the toxin, the body already has antibody present to neutralize the toxin and the greater number of antigen specific B cells and Th cells (memory cells) are rapidly activated to produce extremely high levels of anti-toxin antibody (which is the basis of the booster shots in vaccines).

3.3.2 Immune system respond against bacteria.

For a bacteria not sequestered inside of a cell, the first line of defense is the innate immune response: the inflammatory response and macrophage phagocytosis of the bacteria. The purpose of this innate immune response is to hold the infection at bay until the immune response can be activated. Macrophages which have phagocytized bacteria or dendritic cells which have picked up bacterial debris begin to present bacterial antigen segments with MHC II. These cells travel to nearby lymph nodes where they then can present the antigens to the Th cells to begin their activation. Meanwhile, bacterial debris or even whole bacteria present in the lymph (the fluid surrounding the cells of the body) are carried via the lymphatic system to the lymph nodes. This allows for B cells in the lymph nodes to become stimulated and even resident macrophages in the lymph nodes to pick up antigen for presentation to Th cells. The activated Th cells then interact with the activated B cells and eventually the B cells begin to produce massive levels of antibody. This antibody then gets into the blood circulatory system and is carried to the infection site where it can have a number of effects. Antibody binding directly to bacteria can allow macrophages and neutrophils to attach to the antibody to enhance phagocytosis and killing of the bacteria. Antibody bound to the bacteria can also activate the inflammatory system which eventually results in the activation of macrophages to become better bacteria killers and to cause the release of signals which recruit more macrophages, neutrophils, and even T cells from the blood to the site of infection.

In some instances, T_{DTH} cells in the lymph nodes may also be activated by the accessory cells bringing in antigen. These T_{DTH} cells then leave the lymph nodes to seek out the area of infection. Once in the infection area, the macrophages present more antigen to the T_{DTH} cells to induce them to release several powerful inflammation inducing factors. These include factors that recruit more macrophages and neutrophils from the blood into the area, factors that activate the neutrophils and macrophages to become master killers of microbes (this in addition to the virus-specific antibody greatly enhances the macrophage function), factors that provide help for other Th and T_{DTH} cells in the area, and they can help B cell to enhance antibody production.

The end result of these responses is a massive influx and activation of killer macrophages and neutrophils which phagocytize the bacteria, the influx of antibodies which neutralize the bacteria and enhance their phagocytosis, and the activation of the inflammatory response. The invading bacteria is usually destroyed, however host tissue damage may occur in cases of massive infection. Of note, often the induction of the immune and inflammatory response results in the secretion of high levels of activation factors by the macrophages and T cells. As the levels of these activation factors increase, they often induce the production of inflammation suppressing factors by the immune cells and resident cells of the tissues. This, along with the reduction in the levels of antigens or bacteria for stimulation, allows for the down-regulation of the response and the beginning of wound healing.

3.3.3 Immune system respond against viruses.

Viruses present an interesting challenge to the immune response in that these agents have an intracellular phase, in which they are not available to many of the immune response elements, and often an extracellular phase when the virus is shed from an infected cell to spread to and infect nearby cells. Most of the above immune mechanisms (antibodies and T_{DTH}-macrophage responses) can effectively handle the extracellular phase of the virus. Antibodies bind to the extracellular viruses and prevent their binding to or entering other cells, enhance their destruction by allowing macrophages a handle to bind to the bound antibody and induce phagocytosis, and bound antibody can induce the inflammatory response. T_{DTH} type helper T cells can migrate to the site of infection and direct the activation of macrophages to become master killers with a greater phagocytic capacity, produce factors or cytokines which recruit other T cells, macrophages, and neutrophils into the area of infection, help the activation and maturation of CTLs (see below), and, since the T_{DTH} cells are specialized Th cells, they can help B cells to enhance antibody production. In addition, the T_{DTH} cells can secrete a very potent factor, interferon, which induces all nearby cells to turn on their own internal antiviral defense mechanisms to prevent viral replication and help in preventing the spread of the infection.

Yet the above mechanisms generally have no effect on the viruses hidden within infected cells. The result is that the infection continues because the source (the virus infected cell) has not been destroyed and in some cases the infection can spread via direct cell-to-cell transfer of the virus without an extracellular phase. The destruction of the virus infected cells requires the action of the antigen specific CTLs. CTLs activated at the site of the virus infection can receive immediate help from the T_{DTH} type Th cells in the area to become mature,

active CTLs to kill the virus infected cells. This also releases any internal viruses to be exposed to antibody and macrophages for destruction. Finally, CTLs also can produce interferon which induces more nearby cells to turn on their internal antiviral mechanisms.

The overall effect is that the virus spread and source of infection is stopped. Of course large numbers of memory B cells, T_{DTH} type Th cells, and CTLs are also produced so that in subsequent encounters with the same virus, the specific immune response is very rapid and much stronger; hence, immunity.

3.3.4 Whole body responses to infections.

In addition to the above described immune responses to infectious agents, several other mechanisms are induced which can help in preventing the spread of the infectious agents to different parts of the body.

One of the most striking features of the immune system is that the immune response cells are not centralized, but are spread out in strategically placed lymph nodes throughout the body. The fluids collected from around the cells in only a defined section of the body pass through any single lymph node (e.g. the lymph nodes of the groin area filter fluids from various sections of the legs). These lymph nodes provide a staging area for the interactions which are required for the immune response to occur, interactions which could not occur in the rapidly flowing blood or most normal tissues where the immune cell numbers would be too low. To ensure that the antigens of the infectious agents get to the lymph nodes (often well before the antigens or viruses and bacteria actually reach the lymph node on their own), the macrophages and dendritic cells at the infection site specifically migrate to the local nodes carrying samples of any infection in the tissues. This way, the immune system does not have to initially seek out the infection - it is brought to the immune system. The lymph nodes also provide a filter where lymph node macrophages remove many of the bacteria and viruses from the fluids to prevent the spread of the infection. Indeed, several lymph nodes may be strung in succession to ensure the filtering of infectious agents. Thus, the immune response is localized and direct for a specific area of the body.

However, the results of the localized lymph node immune response is disseminated throughout the body. Antibodies and infection-seeking activated T_{DTH} cells and CTLs quickly reach the blood circulatory system and are spread throughout the body to prevent the spread of the infection. As mentioned above, these cells are actively recruited to the areas of infection by the factors produced as a result of the inflammatory response and activated immune cells. After the close of the immune response, the memory B and T cells continue to migrate throughout the body, spending varying amounts of time in each lymph node on the way. This insures that the memory cells will then be (or soon will be) at the appropriate lymph node to respond to a second encounter with the antigen wherever it may occur.

4. BIOLOGICAL APPROACH TO SYSTEM INFORMATION SECURITY (BASIS)

A modern information security system (ISS) is considered as a number of independent, largely autonomous, network-based, specialized software agents operating in a coordinated and cooperative fashion designated to prevent particular kinds of threats and suppressing specific types of attacks. The modern multi-agent system technology presents a valuable approach for the development of an ISS that, when implemented in a distributed large scale multi-purpose information system, is expected to have important advantages over existing computer security technologies.

There are several principles of the immune system [13] that can be applicable to information security. These principles can make ISS more robust and reliable.

Distributability. There is no central or master cell/organ that is in charge of diagnostic of foreign cells, distribution and reproduction of antibodies, and immune system memory. This in turn implies that there is no single point of failure. This is a very desirable feature for ISS, since it not only avoids bottlenecks and vulnerability but also provides faster response and robustness. A multi-agent approach is able to accomplish this feature/principle for ISS.

Multi-barrier/mechanism. The immune system has multiple barriers or mechanisms to prevent an intruder cell to get in the body and cause harm. A foreign cell will face multiple barriers to penetrate and damage a body. ISS should have different mechanisms to deal with an undesirable piece of software. A combination of these mechanisms could render a highly effective security system.

Diverse mechanisms. Having different mechanisms greatly help the vulnerability of the immune system. These mechanisms may react to a similar antigen in a different way. Each mechanism has its vulnerable/weak points; however, the immune system as a whole is robust. A multi-agent ISS should have diversity in its agents to reduce vulnerability.

Self-rule (autonomous) cells. Most of the cells in the immune system require no management from other places. Each cell with its own mechanism determines the proper reaction to a foreign cell or request from other cells. This feature helps a great deal in providing a fast reaction to an attack and finding a proper response. As

mobile code becomes more common practice, autonomous agents will be required to have a more effective treatment of undesirable software codes.

Adaptability and memory. The immune system is capable of recognizing new antigens and figure out the proper response. The immune system is also capable of remembering antigens that it has dealt with before. The immune system constantly makes a sp ace/time tradeoff in its detector set; at a given time the system maintains a sample of its detector set. In ISS, it is difficult to recognize a new threat. An ISS should be able to learn how to detect new threats based on previous experiences. New threats may be recognized by their abnormal behavior. The agents that have been more successful in combating attacks should be kept and update while agents with no success should be either set in resting place (store) or mutated to have new agents.

4.1 Main BASIS components.

Conceptually, a multi-agent ISS is viewed as a cooperative multitude of the following types of agents distributed both across the network and on the host computer itself [3]. The basic agents include:

(1) A*ccess control agents* that constrain access to the information according to the legal rights of particular users by realization of discretionary *access control rules* (ACR) specifying to each pair "subject - object" the authorized kinds of messages. Various access control agents cooperate for the purpose of maintaining the compliance with discretionary ACR on various sites of network. These agents supervise the flows of confidential information by realization of *mandatory ACR* not admitting an interception of confidential information. These agents act as part of the computer network's *skin* or innate system response.

(2) A*udit and intrusion detection agents* detecting non-authorized access and alerting the responsible system (agent) about potential occurrence of a security violation. As a result of statistical processing of the messages formed in the information system, these agents can stop data transmission processes, inform the security manager, and specify the discretionary ACR. A statistical learning process, crucial for the successful operation of these agents, is implemented. It utilizes available information about normal system operation, possible anomalies, non-authorized access channels and probable scripts of attacks. These agents are used as part of the computer network humeral response. Here agents that have proved to be successful are kept active while the others are either discarded or stored.

(3) *Anti-intrusion agents* responsible for pursuing, identifying and rendering harmless the attacker. Anti-intrusion agents are the parallel of antibodies in the immune system. These agents use knowledge about potential attackers in a similar fashion that an antibody can recognize an antigen. Once the attacker is identified the agent neutralizes it. It should be pointed out that there is no buddy system in our approach as in the immune system with a Helper T lymphocyte (Th) cell.

(4) *Diagnostic and information recovery agents* assessing the damage of unauthorized access. These agents can be seen as part of the cell-mediated response of the computer network system. Here the agents assess the damages (or potential damages) and prescribe an appropriate response.

(5) C*ryptographic, steganography and steganoanalysis agents* providing safe data exchange channels between the computer network sites. These can be seen as part of the way the immune system communicates with different cells (and organs). Here is important to stress the importance of reliable communication between nodes in the network, since agents are distributed all over the network. Thus, access to the proper agent depends greatly on a reliable communication channel.

(6) *Authentication agents* responsible for the identification of the source of information, and whether its security was provided during the data transmission that provides the identity verification. They assure the conformity between the functional processes implemented and the subjects initiated by these processes. While receiving a message from a functional process, these agents determine the identifier of the subject for this process and transfer it to access control agents for realization of discretionary ACR. In is extremely important to set apart self and non-self messages; authentication agents need to use immune system techniques to achieve this task.

(7) *Meta-agents* that carry out the management of information security processes, facilitate coordinated and cooperated behavior of the above agents and assure the required level of general security according to some global criteria.

It could be observed that functions of a number of ISS agents are consistent with the specific functions performed by the components of the biological immune system. Since verbal definitions of the above problems are well established, the BASIS team will utilize its expertise in modern immunology to detect similar tasks performed by the immune system and to establish the qualitative and mathematical description of the relevant immune problems. When applicable, "immune" algorithms will be formalized, implemented in software and subjected to thorough investigation. While this paper presents only an outline of the proposed research, consequent publications will feature current and future effort in this direction.

4.2 Genetic scheme

In our approach we intend to use other biologically inspired solutions such as genetic schemes. Each of the messages that enter in the network will be assigned a genetic print that is based on its message id, destination, type of commands (system calls), and sequence of commands. As a message enters into the network, its genetic print (chromosome) is generated by the host computer. This host computer uses a fitness function to message's chromosome to determine if the message is suited to enter into the network. If message is not fit to enter the network, this message is analyzed further to determine if it is indeed an undesired message. If the message is found to be an authorized one, the fitness function needs to be modified to allow evolution to take place; otherwise, this message is discarded. The host computer analyzes trends in the chromosomes to detect potential large number of "clones" in this population. The host computer collects a representative chromosome sample and sends it to other hosts in the network. This approach will allow the network to identify a large number of clones that come from different parts of the network. This in turn helps to prevent denial of service problems.

The fitness function is modified to allow new applications to be part of the system. As new applications become dominant in the network, the system should learn to let these applications to pass messages in the network. Thus, learning is be accomplished by allowing the fitness function be modified. Since the population (messages) is constantly changing, it is extremely important to include a flexible fitness function to allow changes in different generations. If a message does not meet the fitness function requirements, this is analyzed by a meta-agent to determine if indeed this message is a dangerous one. If the message is determined as a non-dangerous the fitness function needs be modified.

Having a genetic scheme could be seen as a buddy system (along with an immune system scheme) to information security. This buddy system could add robustness to information security, since due to its diversity more potentially attacks can be detected.

5. CONCLUSION

In this paper, we have presented a biological approach to deal with information security on a heterogeneous network of computers. This approach involves a distributed multi-agent scheme along and a genetic approach. This scheme provides implements a buddy system where the two approaches complement each other and provide a better information security system.

ACKNOWLEDGEMENT

The authors are grateful to the Air Force Research Laboratory at Rome NY for funding this research.

REFERENCES

[1] S. Forrest, S. A. Hofmeyer, and A. Somayaji, "Computer Immunology," *Communication of the ACM*, vol.40, No.10, pp.88-96, October 1997.

[2] J. Balasubramaniyan, J. Garcia-Fernandez, D. Isakoff, E. Spafford, and D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents," *In Proceedings of the 14th Annual Computer Security Applications Conference*, Phoenix, Arizona. December 7-11, 1998.

[3] T. R. Gruber, "Toward Principles for the Design of Ontologies used for Knowledge Sharing," *In Proceedings of International Workshop on Formal Ontology*, March 1993.

[4] Hochberg, et al. "NADIR: An Automated System for Detecting Network Intrusion and Misuse," *Computers and Security*, vol.12, No.3, 1993, pp.235-248.

[5] T. Lunt et al., "Knowledge-based Intrusion Detection," In Proceedings of 1989 Governmental Conference Artificial Intelligence System, March, 1989.

[6] P. A. Porras, and P.G. Neumann, "EMERALD: Event monitoring enabling responses to autonomous live disturbance," In Proceedings of 20-th National Information System Security Conference, National Institute of Standards and Technologies, 1997.

[7] S. Stainford-Chen, et al., "GrIDS: A Graph-based Intrusion Detection System for Large Networks," In Proceedings of the 19th National Information System Security Conference, Vol.1, National Institute of Standards and Technology, pp.361-370, October, 1996.

[8] S. J. Stolfo, A.L. Prodromidis, S. Tselepis, W. Lee, D. W. Fan, and P .K. Chan. "Jam: Java agents for meta-learning over distributed databases," In Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, pp.74-81, Newport Beach, CA, 1997.

[9] G. White, E. Fish, and U. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System," IEEE Network, pp.20-23, January/February 1996.
[10] D. Dasgupta (Ed.), Artificial Immune Systems and Their Applications, Springer-Verlag, 1999.
[11] M. Stillman, C. Marceau, and M. Stillman, "Intrusion Detection for Distributed Applications," Communications of the ACM, Vol.42, No.7, pp63-69, July 99.
[12] C. Warrender, S. Forrest, and B. Pearlmutter, "Detecting Intrusions Using System Calls: Alternative Data Models," IEEE Symp. on Security and Privacy, pp133-145, 1999.
[13] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a Computer Immune System," *1997 New Security Paradigms Workshop*, pp. 75-82, Langdale, Cumbria, UK, 1997.