Network Immunity: What can we Learn from Nature for Network Protection?

Michael Kleis
Fraunhofer Institute FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
michael.kleis@fokus.fraunhofer.de

Thomas Hirsch
Fraunhofer Institute FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
thomas.hirsch@fokus.fraunhofer.de

Tanja Zseby
Fraunhofer Institute FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
tanja.zseby@fokus.fraunhofer.de

ABSTRACT

In this paper we analyze Network Immunity as a bio-inspired approach for detecting anomalies in communication networks. We briefly review the basic methods of Artificial Immune Systems (AIS), identify their strengths and weaknesses, and evaluate their possible applications to intrusion detection in computer networks. After an overview of related work from the area of intrusion detection we collect key challenges anticipated for the realization of Network immunity based on AIS.

Keywords

Network Intrusion Detection, Artificial Immune Systems, Survey, Anomaly Detection

1. INTRODUCTION

Despite a lot of research in this area, network security is still one of the largest challenges in computer networks. Network attacks can cause serious damage at global scale and endanger the operation of the Internet. The best, fastest and most efficient network is worth nothing if attackers can gain control. The monetary loss from Internet attacks can be immense. In addition, attacking network infrastructure and end systems has already become instrument in warfare and organized crime. So it does not come as a surprise that security is often the number one target objective in future network design approaches like autonomic communication and other post-IP approaches. In this paper we investigate to which extent we can adopt and incorporate methods that have evolved in nature in order to achieve better security in computer networks. We here concentrate on particular methods of the Human Immune System (HIS). We point out the main principles and analyze differences and commonalities between the challenges and conditions in biological systems and those in computer networks. Based on this we investigate the applicability of biological principles to future networks.

Bionetics '07, December 10-13, 2007, Budapest, Hungary

2. FROM INTRUSION DETECTION TO NETWORK IMMUNITY

Threats to network security range over a broad scale, they may originate from "script kiddies" hardly aware of the havoc they create and the liabilities they might face, up to purposeful criminal acts of organized crime and terrorism, or the attacks from foreign intelligence and part of warfare. Under such hostile environments, Intrusion Detection becomes a crucial part of network protection and security. Detection methods can be classified in two main categories:

- *Signature detection* is based on known attack signatures. In general, such systems can provide low false positives, but of course, the detection power is limited to known attacks only.
- *Anomaly detection* detects changes in the system behavior; however, the classification into valid and malicious changes is difficult, therefore it result in high false positives, and require frequent human intervention.

Current detection methods available on the market mostly concentrate on signature based methods (e.g. virus scanners, intelligent firewalls). They work well for known attacks, but fail to detect unknown attacks (zero-day). Therefore, they may easily be outsmarted by attackers using slightly modifying attack signatures[11][14]. In an era where the time span from the disclosure of a security hole to its exploit has decreased to a few hours, approaches that work for zero-day detection become an urgent need. This is even becoming more pressing, as yet undisclosed security holes are traded with high value on the black market, where typical buyers include intelligence agencies and organized crime[13].

One of the main weak points of intrusion detection is that the system can be flooded with false alarms. At the same time, single attacks often generate multiple alerts. Current IDS face the challenge to logically group related alerts[4] for

the operators' understanding. Early distributed intrusion detection systems such as DIDS [15], and NetSTAT [16] collected audit data from distributed component systems but analyzed them in a central place. However, the scalability of such systems is limited due to the central analysis[12] Information collected can exceed the processing capacity of any single system, while the collection process congests the network bandwidth. A true immune system on the other hand is heavily distributed in many of its tasks.

[1] presents a cooperative module for IDS. This module provides functions to manage and correlate alerts. The papers show that these functions significantly reduce the number of alerts. However, they also observe that alerts obtained are still too elementary to be easily managed by a security administrator. It presents a centralized layout, with a core server receiving all the alerts provided by the IDS. A more distributed approach was presented in [17]. The authors illustrate their approach with the Mitnick attack in a two-step procedure. The approach is closely related to this attack type.

To address the issues of scalability and distribution, we propose Network Immunity as a bio-inspired approach for detecting anomalies in communication networks. That is we investigate to which extend we can adopt and incorporate methods that have evolved in nature in order to achieve better security in computer networks. We here concentrate on particular methods of the Human Immune System (HIS). In general it is assumed that the purpose of the HIS is to protect our body from the ever-changing onslaught of biological and biochemical entities (pathogens)[7][8]. The overall structure of the Immune System is comparable to a multilayered system. Each layer corresponds to a line of defence and the core layers can be summarized as follows:

- **Skin:** Physical barrier to the body for pathogens.
- **Physical Conditions:** E.g. pH-Value and temperature of the body.
- **Innate Immune System:** A set of roaming scavenger cells (e.g. phagocytes) we are born with.
- **Adaptive Immune System:** A system of B and T-Cells (lymphocytes) that is able to adapt to, and learn the structure of new pathogens.

The layer of the Adaptive Immune System is of particular interest from the viewpoint of Network Intrusion Detection because of its capability to detect and defend previously unseen attacks with a very high success rate. In addition, the Adaptive Immune System operates in a parallel and distributed manner with partial decentralized control mechanisms, while implementing features as pattern recognition for self/nonself discrimination, adaptation, (associative) memory and learning[2].

3. ARTIFICIAL IMMUNE SYSTEMS

As a new branch of Computational Intelligence (CI), *Artificial Immune Systems (AIS)* emerged in the 1990s[2]. AIS related methods restrict themselves mainly on the study of immune abstractions[7]. That is, they focus on exploring various single functions known from HIS. In Figure 1 we provide an overview of selected functions of the Adaptive Immune System, corresponding AIS Models and some of the AIS algorithms developed. For the AIS Models shown we focus on *Negative Selection Algorithms*, *Clonal Selection* as well as *Immune Network Models* which are the most discussed ones following[2]. In the remainder of this section, we will briefly describe each model.

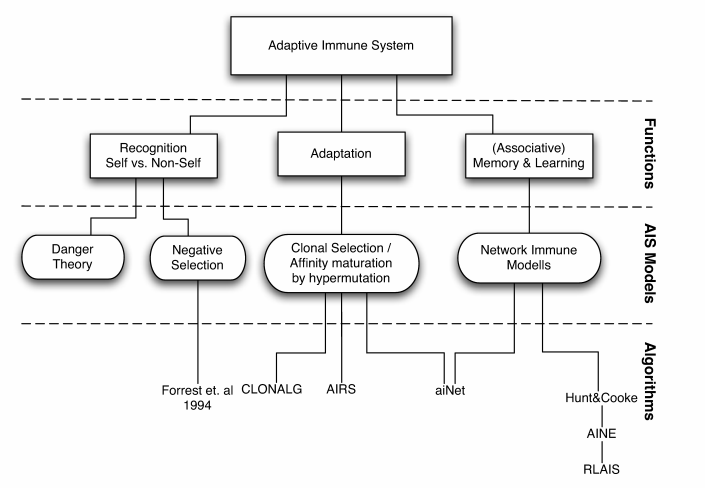

Figure 1: Selected Functions of the Adaptive Immune System

3.1 Negative Selection

A precondition for a working Immune System is self tolerance. For this reason it is e.g. required to prevent the production of autoreactive B-Cells, i.e., B-cells that would react with cells that belong to the own organism. The strategy used for this task is the so called Clonal Deletion or Negative Selection principle. The underlying principle of Negative Selection has been described by Forrest et al.[5] as follows: In a first step a set of detectors is generated by a random process. Then each potential detector is brought together with the elements of a set containing samples of self structures. Those detectors that match samples of the self-structure (i.e. react with elements belonging to the own organism) are eliminated. The remaining set are those that do not react to own elements. Those are added to the detector set (negative selection). At the actual detection step a sample item is compared with the detectors and in case of a match it is classified as non-self.

As one feature of this approach it is not required to know an antigen signature in advance to be able to detect it. Projected into the networking domain this corresponds to the fact that Negative Selection based Intrusion Detection has the potential to detect even zero day attacks. Since this would be a definite progress beyond the state of the art in signature based Intrusion Detection, one research question addressed for Network Immunity is: "How can we utilize Negative Selection for Intrusion Detection in a resource efficient manner?".

3.2 Clonal Selection

Main actors of the Adaptive Immune System are B-Cells, which are equipped with specialized weapons to fight different kind of enemies. When a B-Cell recognises an antigen it starts cloning itself and secrets free antigens. The process of amplifying only those cells that produce useful antibodies is

called clonal selection. Clones are subject to somatic mutation (to increase diversity) and the rate of cloning a B-Cell is proportional to its "fitness" to the problem: I.e. fittest cells replicate most. CLONEALG[3] is one example for an Algorithm based on the described Clonal Selection principle which can be e.g. applied to pattern recognition problems.

Mapped into the computing domain, clonal selection for affinity mutation has a strong relation to the field of mutation based, evolutionary algorithms. In fact, clonal selection has successfully applied to pattern recognition, data analysis and optimization problems[2]. Beneath this areas of application, with Network Immunity we also address the research question: "Can we use clonal selection to infer defense strategies for new, unknown attacks based on past knowledge?".

3.3 Immune Network Models

Immune Network Models are based on the hypothesis that biological Immune systems maintain an Idiotypic Network to realise an (associative) memory as well as learning[10]. The underlying core of this hypothesis is, that even in the absence of foreign antigens, B-Cells are interacting which each other. The sum of this interactions forms the before mentioned Idiotypic Network. For a comparative survey of artificial immune network models see e.g.[6].

The realization of learning and associative memory functions comparable to the ones of biological immune systems is anticipated as one core requirement for Network Immunity. We therefore propose to investigate in utilization of Network Immune Models to realize a (distributed) defense strategy database(DSDB) concept. Conceptionally, the DSDB maintains the information what defense strategy to apply in case a concrete attack pattern is observed, in order to react to previously unkown attacks. The DSDB should include support for similarity and associative search functions.

4. NETWORK IMMUNITY CONCEPTS

Based on the AIS models described above we postulate a set of concepts that should be realized in order to build a system to achieve Network Immunity. In the following we will list each concept and provide a relation to the HIS or AISs.

- **Situational Awareness**: In nature the behaviour of new B-cells is observed in order to provide a basis for the selection process. Based on the observation only the best performing B-cells are duplicated.

- **Information Sharing:** B-cells interact with each other and realize memory functions (e.g. by realizing an Idiotypic Network).

- **Mutation and Learning:** Any a-priori knowledge about potential attacks can help. In medicine vaccination is used to transfer knowledge gained from one system into another system. In most cases only the second system can be saved and victims needs to be sacrificed to gain this knowledge. Good strategies (well performing B-cells) are slightly modified in order to increase their variability to be prepared for new attacks.

- **Self-Tolerance:** Discriminate between Self and Non-Self prevents the accidental destruction of own elements by too aggressive defense strategies.

5. APPLICABILITY TO NETWORK INTRUSION DETECTION

Before one can apply immune system methods for intrusion detection, it is required to specify how the biochemical processes of an biological immune system can be mapped into the computing domain. In addition it is not obvious if the dynamics of network traffic are comparable with the variability inside the human body. Thus the problem specific selection of data and detector representations, data matching techniques (e.g. similarity vs. exact matching), metrics and feature vectors are just a few examples of challenging tasks.

Given that these tasks are completed, in computer networks it is reasonable to run multiple strategies in parallel as well. E.g. many signatures of intruders are known in advance and can be easily recognized and eliminated. Detection techniques based on know signatures would correspond to a part of the innate immune system are nowadays widely deployed in the form of virus scanners and advanced firewall systems. Nevertheless, recognition of specific signatures, can only be applied to known attacks. Thus previously unknown, so-called zero-day attacks remain undetected. Anomaly detection methods on the other hand analyze statistics of relevant metrics, such as network traffic or system call data, to detect unusual changes in the systems behavior. Those techniques correspond to the strategies of the adaptive immune system.

Distribution and information sharing is essential in immune systems. Such cooperation among network nodes and neighbor networks is also useful in network security strategies. It helps not only to share resources for data capturing and analysis but also allows to combine multiple viewpoints. Therefore we consider this as one key component that helps to make increase security in computer networks. Also learning from the past is a useful strategy in network security. Knowledge can be derived from previous attacks or from attacks that happened in other networks. Similar to principles in human medicine attacks can be re-directed to less critical systems (honeypots) in order to learn the signatures and provide resistance for more critical network components in future.

A significant difference between biology and computer networks can be seen in the attack design. In biology most viruses are a result of a evolutional process. In contrast to this, attacks for computer networks are designed by humans. Therefore some information can be derived from a-priori assumptions about the attackers incentives. E.g. incentives to perform an attack, most attractive attack targets, available resources, degree of destruction aimed at, etc. These facts can be exploited to help to envision the look of future attacks.

Random mutation and selection help to improve the HIS step-by-step. This trial and error method is a very time- and resource-intensive process. In computer networks we have the possibility to use external control to speed up the process by using knowledge from the past and by common sense (e.g. about attackers incentive). With this information we can substitute random mutation by more directed algorithms. Furthermore, when applying biological principles to computer networks we have to keep in mind that the human immune system is not invulnerable.

Also in computer networks one need to ensure that the de-

fense and protection of a system does not open new security vulnerabilities (e.g. overloading an adaptive measurement system by just simulating an attack).

5.1 Potential contribution to Intrusion Detection

Network Immunity will focus on a intrusion detection system that is based on parallel and partly (distributed) immune system methods for pattern recognition, memory, Self and Non-Self discrimination and learning. Since it could be shown that peer-to-peer notification mechanisms improve the speed and scalability of IDS alert propagation[9], a combination of AIS methods and principles known from area of peer-to-peer systems will be one promising starting point towards the realisation of a functionality for detection of distributed attacks and correlation of attack patterns. As anticipated results of Network Immunity related research, we see a potential for a progress beyond the state of the art with regard to the following topics:

1. **Detection of Unknown (zero day) or modified attacks:** For Network Immunity we propose to investigate in the applicability of the Negative Selection principles for intrusion detection. This is of interest, since a Negative Selection based Intrusion Detection has the potential to detect zero day attacks. Further affinity mutation or clonal selection principles known from AIS may act as tool to detect modified attacks.

2. **Learning of, and disseminating knowledge about attacks and corresponding defense strategies:** The Network Immunity approach combines state of the art intrusion recognition with inter-IDS communication to provide other systems a view of current, rather than past, anomalies. Archetypes in this context are Immune Network Models. A (Distributed) Defence Strategy Database based on P2P principles can act as an associative memory for Network Immunity.

3. **Mapping of biological principles to Networking Domain:** For Network Immunity we have to focus on the problem specific selection of data and detector representations, data matching techniques (e.g. similarity vs. exact matching), metrics and feature vectors. Having a strong focus on network security we expect several improvements with regard to the application of AIS to network security domain.

6. CONCLUSIONS

Immune systems are highly distributed, and rely on that distribution to be effective. As with the multitude of antigens in the human body, they rely on the parallel processing power of biological systems to become effective classifiers. We assume therefor that a distributed system, with active communication of successful attack patterns between detectors will best realise the HIS' distributed pattern detection. Moreover, the HIS components are specialized either to detect, memorize, or fight intruders. This specialisation will also be efficient in the network context. Detectors at the edge of the network, on end user systems, where detection is easiest, communicating with each other. Centralised attack databases in the bone marrow of the network, can correlate alerts. Firewalls represent the B-Cells, employing filter patterns which have been agreed on.

7. REFERENCES

[1] F. Cuppens and A. Miège. Alert correlation in a cooperative intrusion detection framework. In *SP '02: Proceedings of the 2002 IEEE Symposium on Security and Privacy*, page 202, Washington, DC, USA, 2002. IEEE Computer Society.

[2] D. Dasgupta. Advances in artificial immune systems. *Computational Intelligence Magazine, IEEE*, 1(4):40–49, 2006.

[3] L. N. de Castro and F. J. V. Zuben. The clonal selection algorithm with engineering applications. In *Artificial Immune Systems*, pages 36–39, Las Vegas, Nevada, USA, 8 2000.

[4] H. Debar and A. Wespi. Aggregation and correlation of intrusion-detection alerts. In *RAID '00: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, pages 85–103, London, UK, 2001. Springer-Verlag.

[5] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri. Self-nonself discrimination in a computer. In *SP '94: Proceedings of the 1994 IEEE Symposium on Security and Privacy*, page 202, Washington, DC, USA, 1994. IEEE Computer Society.

[6] J. C. Galeano, A. Veloza-Suan, and F. A. González. A comparative analysis of artificial immune network models. In *GECCO '05: Proceedings of the 2005 conference on Genetic and evolutionary computation*, pages 361–368, New York, NY, USA, 2005. ACM Press.

[7] S. M. Garrett. How do we evaluate artificial immune systems? *Evol. Comput.*, 13(2):145–177, 2005.

[8] S. A. Hofmeyr. *An Interpretative Introduction to the Immune System.* Oxford University Press, 2000.

[9] W.-Y. Hsin, S.-S. Tseng, and S.-C. Lin. A study of alert-based collaborative defense. pages 6 pp.–, 2005.

[10] N. Jerne. Towards a network theory of the immune system. *Ann Immunol (Paris)*, 125C(1-2):373–89, January 1974.

[11] E. Levy. Approaching zero [attack trends]. *Security & Privacy Magazine, IEEE*, 2(4):65–66, 2004.

[12] P. Ning, S. Jajodia, and X. S. Wang. Abstraction-based intrusion detection in distributed environments. *ACM Trans. Inf. Syst. Secur.*, 4(4):407–452, 2001.

[13] H. Pohl. Zur technik der heimlichen online-durchsuchung. *Datenschutz und Datensicherheit*, 9/2007, 2007.

[14] D. N. Serpanos and C. Douligeris. *Network Security.* Wiley-IEEE Press, 2007.

[15] S. Snapp, J. Brentano, and G. Dias. Dids (distributed intrusion detection system) âĂŞ motivation, architecture, and an early prototype. 1991.

[16] G. Vigna and R. A. Kemmerer. Netstat: A network-based intrusion detection system. *Journal of Computer Security*, 7(1), 1999.

[17] J. Yang, P. Ning, X. S. Wang, and S. Jajodia. CARDS: A distributed system for detecting coordinated attacks. In *SEC*, pages 171–180, 2000.