'DNA-proofing' for computer systems - a new approach to computer security?

C.P.LOUWRENS, S.H. VON SOLMS
Department of Computer Science, Rand Afrikaans University, P.O. Box 524, Auckland Park, Johannesburg, 2006, South Africa.
Telephone: *+27 11 489 2843*
Fax: *+27 11 489 2138*
E-mail: buksl@nedcor.co.za , basie@rkw.rau.ac.za

Key words: Computer security, DNA-proofing, anti-virus technology, biological model, immune system, autonomous intelligent software agents.

Abstract: Modern day network-centric computing can increasingly be viewed as a vast, extremely involved organism, of which the boundaries are not clear, and most of the constituent parts are unknown from any given viewpoint. It may even become impossible to ensure the security of computing systems in future with current approaches to computer security. On the other hand, nature has been successful in defending its complex biological systems from infection and damage for countless millennia by using highly specialized and evolved immune systems. It is therefore postulated that a highly effective defensive mechanism can be developed, to transparently enforce an acceptable level of security in very extensive and complex computer networks and systems, by building very basic, but specialized autonomous agents, that follow basic rules that can be deduced from biological immune systems. Key to this concept is the biological system's ability to distinguish what belongs to it and what is foreign and therefore needs to be destroyed. This is done, inter alia, via genetic information contained in the DNA of each cell. Central to the proposed immune model is thus the concept of 'DNA-proofing'

1. INTRODUCTION

This article is a follow-on of a paper by the same authors presented at the 12th World Congress of the international Federation for Information Processing / Security '98 (IFIP/SEC'98). In the paper, which posed the

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

question if computerized immunity could be achieved based on a biological model, it was concluded that it was indeed possible, but only if we fundamentally change our approach to traditional models of computer security. The proposed model stands the traditional approach to computer security on its head, as it insists that every component in a computer system must be able to be classified as part of the system, or as foreign.

While the concept itself may not be revolutionary (it has existed for countless millennia in the natural world), it may revolutionize the way we approach computer security system design in future. Key to this concept is the biological system's ability to distinguish what belongs to it and what is foreign and therefore needs to be destroyed. This is contained in the genetic information contained in the DNA of each cell. The term 'DNA' (deoxyribonucleic acid) used to describe biological systems has been retained because of its identical use in the proposed computer model, as well as the instant understanding of the concepts it evokes.

The purpose of this paper is thus to propose a model, based on concepts from biological immune systems, whereby computer systems can protect themselves by being able to identify all constituent parts through a proposed system called 'DNA-proofing' and thereby detect and deal with any foreign code or hardware. This paper deals with the subject conceptually and does not concern itself with the details of implementation. This paper is structured as follows:

Part 1 introduces the current and future problems facing computer security, as well as providing some background as to the origin of this paper.

In Part 2 we provide a brief overview of the concepts involved in biological immune systems. This is necessary to enable the reader to understand the analogies proposed in the computer immunity model.

In Part 3, the proposed computer immune model, as well as the essence of the model, namely the concept of 'DNA-proofing' is discussed in detail.

Part 4 consists of the conclusion and final remarks on the possible implementation of the model.

2. BRIEF OVERVIEW OF BIOLOGICAL IMMUNE SYSTEMS

The immune system forms the body's defense against a foreign substance (antigen), whether it is a microorganism (bacteria, fungi, viruses, protozoa and parasites), a potentially toxic material (foreign protein, carbohydrate, or nucleic acid), or an abnormal cell (one invaded by a virus or having become malignant). An antigen is a substance that, when introduced into an organism, induces an immune response consisting of the production of a

circulating antibody (gammaglobulin or immunoglobulin). It attacks the antigen and maintains a memory (antibodies) of the invader so a second exposure will provoke a greater, faster response. If all goes well, the immune system overtakes the bacterium so that the disease is under control. Suppressive, self-regulatory mechanisms then come into play to shut down the immune response (Ling, 1992).

The immune system originates, as with every biological entity, from the genetic code or deoxyribonucleic acid (DNA) inherited from the parents. Contained in the DNA are millions of `codes' relevant to the programming of the immune system to respond to specific antigens. (Bishop, 1991) In addition, some immunity is transferred from the mother to the fetus while in the womb via the placenta, and after birth, further transfer of immunity from the mother to child takes place via breast milk. After this, the baby's Thymus gland starts to manufacture more than 500 billion T Lymphocytes (T cells) which contain the blueprints to recognize more than a million antigens. White blood cells (antibodies) are manufactured in the bone marrow. (Dwyer, 1993) Immunity can also be introduced to a previously susceptible body by applying a weakened form of the antigen (process called inoculation), to evoke an immune response. This technique thus extends and augments the biological immune system (Dwyer, 1993).

3. DNA- PROOFING AS PROPOSED MODEL FOR COMPUTER IMMUNITY

3.1 Introduction

The basic concept of the *DNA-proofing* model is extremely simple: Each computer system must be able to identify every constituent component of that system, without necessarily having to know about, or keep a configuration of the complete system. This can be achieved through a system we shall call *DNA-tagging* (Defined later).

The proposed *DNA-proofing* model for computer immunity consists of four distinct processes, namely: The *verification process, setup process, tagging process,* and the *immune process* as well as two additional entities, the *International Standards and Security Certification Authority (ISSCA)* and *Specialist Immunology Authority (SIA).* Please refer to figure 1 for more detail.

The different processes and entities are now discussed in more detail, starting with the *DNA-tags*, followed by the immune process and other components.

3.2 DNA-tags

The concept of *DNA-tags* is central to the *DNA–proofing* model for computer immunity. This mechanism enables the computer system to identify with certainty, which components belong to it, and which are foreign. This allows the computer immune system to be pro-active in its approach to identify and deal with antigens in the system.

The *DNA-tag* is an extension of the *Proof-Carrying Code (PCC)* technique proposed by Necula et al (Necula, 1998), which enables a computer system to determine, automatically and with certainty, that program code (which could also be an agent) provided by another system is safe to install and execute. The extension involves the addition of a unique code that will identify the computer system to which a tagged component belongs: (hardware, software and data). The *DNA-tag* could also contain the security credentials of users on the system, which allows users to be treated as any other component as part of the computing system. The integrity of *DNA-tags* must be ensured with tamper-evident mechanisms and/ or secure hashing schemes.

3.3 The immune process

The immune process is analogous to the immune system in a biological entity, which must be ever alert and vigilant. Please refer to figure 2 for a graphical depiction of the immune process.

For the moment we will assume that all constituent components (hardware, software and data) have been tagged with a unique code, which serves as the computer system's DNA.

Two types of checking are required for the immune process to take place:

- Firstly, all tags are checked run-time against the DNA-database when required for processing.
- Secondly, roaming agents perform random checks on resources not in active use, like databases or application software.

Should it not be tagged, or should it not have a tag that conforms to the 'DNA' of the system, it is referred for comparison to the antigen database. Should a discrepancy (antigen) be found, it is immediately encapsulated (sand-boxed) to prevent it from being executed and compared with a database of known antigen signatures (similar to a conventional virus signature database).

If the antigen can be identified, the appropriate countermeasures are taken, the antidote applied and the occurrence logged for management information purposes. Should the antigen not be identified, it is then referred to a specialist set of agents who will then analyze the antigen by using a heuristic process. Like its biological counterpart, it is expected that in many cases the antibody agents would be able to devise an antidote without external interference (Louwrens, 1998). The remedy would then be applied and logged. It is worth mentioning that all the activities up to this point has been transparent and has not required any human intervention. This is analogous to the biological immune system being able to cope with an antigen. When the antibody agents cannot identify the antigen (and thus not devise an antidote), a sample of the antigen is then prepared and automatically transported to a *SIA* and the system administrator(s) informed

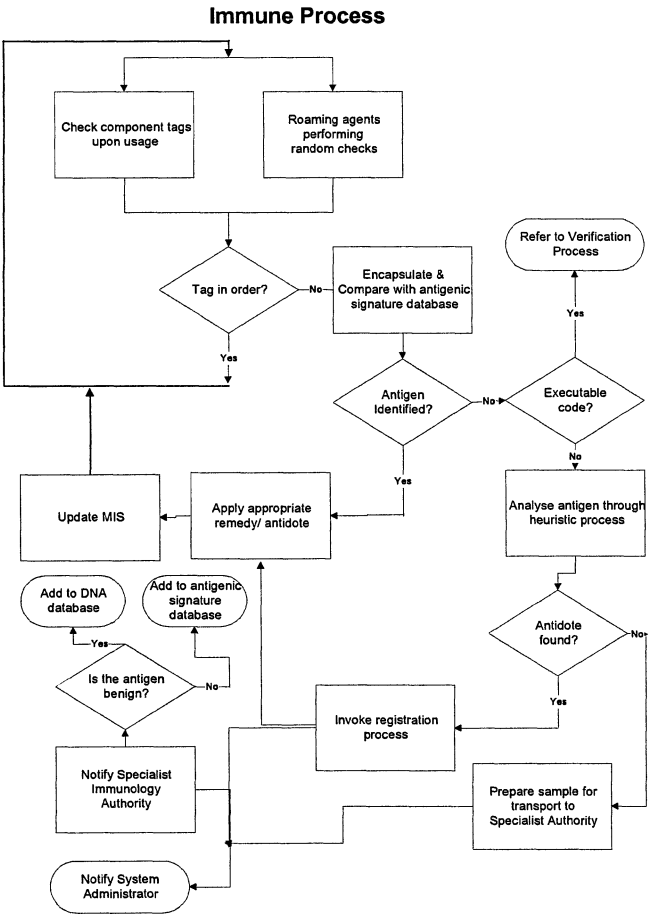

Figure 2: The computer immune process

of the situation. The *SIA* will then use sophisticated means to identify, classify and develop countermeasures for the antigen. If it is found to be benign, it can simply be added to the DNA-database. Should it be harmful, the antigenic signature will be added to the antigenic signature database of all participating computer immune systems.

As can be seen from the process above, the proposed immune system is able to deal with new and previously unknown antigens (viruses) and should be able to deal with most cases in a transparent way.

The integrity of the antigen database is of paramount importance, because 'antigens' that are actually benign system components can be introduced by malicious agents, which can lead to the destruction of perfectly good system components or data. In the biological world this is called autoimmunity.

3.4 Setup, verification and tagging process

The *setup process* effectively bootstraps a new or reconfigured computing system. It is essential that the initializing is done via a *Secure Embryonic Mechanism (SEM)*, which can be allowed to construct the various immune agents (Louwrens, 1998) needed under controlled circumstances and in a secure environment. The *SEM* will use the secure DNA-database to construct and initialize the various immuno-agents needed for the computer immune system. The unique DNA signature for the system will also be generated at this time to be used in the DNA-tagging process.

Every computing system must also have a *verification process* that will perform certification confirmation tests on components (Standard queries must result in predictable results) These tests must in principle be indiscernible from actual transactions to ensure that these answers cannot be spoofed. The checking process is executed within a low risk environment like a trusted computing base within the immune engine.

DNA–proofing adds the additional dimension of also uniquely identifying the computing system it belongs. Every component, node, data item, program, subsystem, etc. must be identified and *tagged* with a *DNA-tag*. This means that hardware components must be able to be tagged as well. It may not be feasible to *DNA-tag* individual components, but analogous to a biological cell – any component that performs an identified useful function (I/O, CPU, communications, routing, drives, screen, etc) must have an identifiable tag which can be associated with the total computing system. Should a new component be added or component be changed, it will be detected automatically, and subjected to the verification and registration process.

3.5 Specialist Immunology Authority (SIA)

The *Specialist Immunology Authority (SIA)* is a facility, which serves as a specialized computer immunology laboratory that deals with situations when the computer systems own immune system cannot cope with the antigen. It adds a collaborative intelligence level to the computer immune system whereby human and custom expert systems can identify, classify and develop antidotes for referred antigens. When antigens are identified, the antigenic signature can be downloaded (after certification by the *ISSCA*) to all participating computer immune systems and these systems can then become effectively 'inoculated' against the particular antigens. Similarly, should the computer immune system be able to identify and devise a cure by using the intelligence within its own immune system, the information can be downloaded to the *SIA* to verify and distribute to participating systems.

3.6 International Standards and Security Certification Authority (ISSCA)

The *International Standards and Security Certification Authority (ISSCA)* is a proposed organization which will regulate the international security standards and certification that is needed for the successful implementation of the *DNA-proofing* model. The role of the *ISSCA* will be to certify that code produced by the code producer (code originator) conforms to the security policy and safety predicate as required by the code consumer (user of the proofing code), similar to the *PCC* proposed by Necula et al (Necula, 1998). It is assumed that international standards would emerge which code consumers would subscribe to, not unlike the "Common Criteria (CC) for Information Technology Security Evaluation" (ISO 15408) that is currently being produced. Every distinct component would become a TOE (Target of Evaluation) and would have to conform to a Protection Profile (PP) as in the CC (CEMEB, 1999). This removes the need for the code consumer to perform these proofs themselves.

The need for certification of hardware and software leads to another basic requirement – namely the development and acceptance of international certification criteria for each type of discrete component. This means that in addition to the interface and technical standards adherence, every component must also be able to be certified in terms of functionality and integrity.

4. CONCLUSION

The proposed *DNA-proofing* model does not require revolutionary technologies, but is instead a novel way of consolidating and implementing several existing and emerging technologies, based on the biological immune system. In the authors' opinion, it is inevitable that there will be future convergence between the traditional models of computer security and biological immune systems.

All biological analogies are not necessarily valid. Furthermore, the issue of complexity begs the question of prevailing capabilities of technology, etc. but with the current rate of development of computer hardware and software, coupled with the quantum leaps in processing power and storage capacity, this can be feasible in 15 – 20 years from now. What is important though, is that certain components of this model can be identified and implemented with immediate effect. Identified concepts should be investigated and developed further as base components, or building blocks for eventual implementation. The proposed or similar solution, may be essential for the survival of computer systems in future.

5. REFERENCES

Bishop, Jerry, E. and Waldholz, Michael, (1991), *GENOME*, Touchstone, Simon & Shuster, New York.

Chess, David M. (1998): *Security Issues in Mobile Code Systems*, in Giovanni Vigna (Ed.), (1998): *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Clark, William R. (1995), *At War Within, The Double-Edged Sword of Immunity*, Oxford University Press, New York.

Dwyer, John, (1993), *The body at war, The story of our immune system,* Second Edition, J M Dent, London.

Ford, Richard, (1999) : *No Surprises in Melissa Land*, Computers & Security, Vol. 18, No. 4, 300-302, Elsevier Science Ltd.

Hohl, Fritz (1998): Time Limited Blackbox Security: *Protecting Mobile Agents From Malicious Hosts*, in Giovanni Vigna (Ed.), (1998): *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Ling, Noel, R.: *Cells of the immune system,* in Klara Miller, John Turk & Stephen Nicklin (Eds) (1992) : Principles and Practice of Immunotoxicology, Blackwell Scientific publications, Osney Mead, Oxford, OX2 0EL.

Louwrens, C.P. and Von Solms, S.H. (1998) *Can computerized immunity be achieved, based on a biological model?* in György Papp; Reinhard Posch (eds.), Global IT Security, Proceedings of the XV.IFIP World Computer Congress 31 August – 4 September 1998, Austrian Computer Society, Wollzeile 1-3 1010 Vienna, Austria.

Miller,Greg,(1997), *Anti-virus technology moves forward,* CNN Sci-Tech, http://www.cnn.com/TECH/9710/21/anti.virus.technology.lat/ , October 21, 1997.

Necula, George C. and Lee, Peter (1998): *Safe, Untrusted Agents using Proof-Carrying Code* in Giovanni Vigna (Ed.), (1998) : *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Riordan, James; Schneider, Bruce (1998): *Environmental Key Generation Towards Clueless Agents*, in Giovanni Vigna (Ed.), (1998): *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Sander, Thomas, Tschudin, Christian F. (1998): *Protecting Mobile Agents Against Malicious Hosts*, in Giovanni Vigna (Ed.), (1998): *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Shimson Berlowits, Joshua D. Guttman, Vipin Swarup (1998): *Authentication for Mobile Agents*, in Giovanni Vigna (Ed.), (1998) : *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

Steels, Luc, (Ed),(1995): *The Biology and Technology of Intelligent Autonomous Agents*, NATO ASI Series, Series F: Computer and Systems Sciences, Vol. 144, Springer-Verlag, Berlin.

The Common Evaluation Methodology (CEM) Editorial Board (CEMEB)(1999): *Common Criteria (CC) for Information Technology Security Evaluation*, ISO/IEC 15408-1: 1999 (E), http://csrc.nist.gov.

Vigna, Giovanni, (1998): *Cryptographic Traces for Mobile Agents*, in Giovanni Vigna (Ed.), (1998): *Mobile Agents and Security*, Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, ISBN 3-540-64972-9.

6. BIOGRAPHY

Cecil (Buks) Louwrens is currently a Ph.D. student at the Department of Computer Science of the Rand Afrikaans University in Johannesburg, South Africa. He is also a senior manager in Nedcor Bank in South Africa.

Professor Sebastiaan (Basie) von Solms is Head of the Department of Computer Science at the Rand Afrikaans University in Johannesburg, South Africa. He is also the South African representative on Technical Committee 11 [Information Security] (TC11) of the International Federation for Information Processing (IFIP), and is present Chairman of TC11.

Prof von Solms has published numerous research papers on Information Security. He is also a member of the Review Panel of the journal Computers and Security, as well as a member of the Editorial Board of the South African Computer Journal.