



# Security Analysis in Internet Traffic through Artificial Immune Systems

---

Workshop “Thrustworthy Software”

Michael Hilker

University of Luxembourg, Campus Kirchberg  
Interdisciplinary Lab for Intelligent and Adaptive Systems  
Management of Information and Net-Centric Computing Group  
6, Rue Richard Coudenhove-Kalergi, L-1359 Luxembourg

e-mail: [michael.hilker@uni.lu](mailto:michael.hilker@uni.lu) phone: +352-466644-5311



# Agenda

---

- Who am I
- Introduction
- SANA
  - Artificial Immune System
  - Artificial Cells
- Architecture, Scenarios and Results
- Next Steps
- Conclusion



# Who am I

---

## Michael Hilker

- PhD-Candidate at the University of Luxembourg, supervised by Prof. Dr. Christoph Schommer, funded through a Scholarship of Luxembourg.
- Computer Scientist, graduated at the Johann Wolfgang Goethe-University Frankfurt, Germany in March 2005
- Working in the fields Biological Inspired Computing, Artificial (Immune) Systems, Intrusion/Anomaly Detection, Adaptive Systems, and Ant Colonies



# Introduction

---

- Networks are under a constant Assault from Intrusions, e.g. Viruses, Worms, Trojans.
- Infected Computers cause
  - high costs for removing the infection
  - often a stop for the usage of the computer
  - a risk for infection other machines
- Network Intrusion Detection Systems (NIDS):
  - Centralised, Semi-Automatic and Local Systems
  - Need plenty of Computational Power



# Introduction

---

- NIDS run on a Server – e.g. E-Mail-Server or Internet-Gateway.
- They use a huge Database with known Attacks and how to identify and prevent these known Attacks.
- They only observe the Network-Traffic routed over this Server in order to prevent Attacks.
- They do not identify the following Attacks:
  - Attacks which are not routed over the NIDS, e.g. USB-Stick or additional Internet-Connection
  - Unknown Attacks – either new or modified
  - Disguised Attacks
  - Overload – if there is too much traffic, the NIDS cannot check all Traffic because it needs too much computational power.



# Introduction

---

- Consequently, novel Approaches for Network Security are needed.
- The following Features are required:
  - Distributed, secures the whole Network
  - Computational Power is shared over the Network
  - Adaptive, learns how to detect new Attacks
  - Autonomous, works without central center



# Immune System

---

- Human Immune System (HIS)
- Protect the Human Body against Pathogens. It works efficient, unsupervised and it adapts quickly to new Pathogens. Additionally, it protects the whole body and each Component works autonomously.

“Nearly perfect Security-System for the Human Body”
- Building an Artificial Immune System (AIS) with the Advantages of the Human Immune System would enhance current NIDS.



# AIS – Artificial Immune System

---

- Artificial Cells – Agents – flow through the Network and perform Task in order to guarantee the Network Security.
- Some Features of Artificial Cells:
  - Lightweighted, Mobile
  - Autonomous
  - Adaptive
- Examples of Tasks:
  - Evaluate Packets whether they contain an Attack or not
  - Observe Status of a Network Node
  - Monitor Statistical Data about Network Traffic



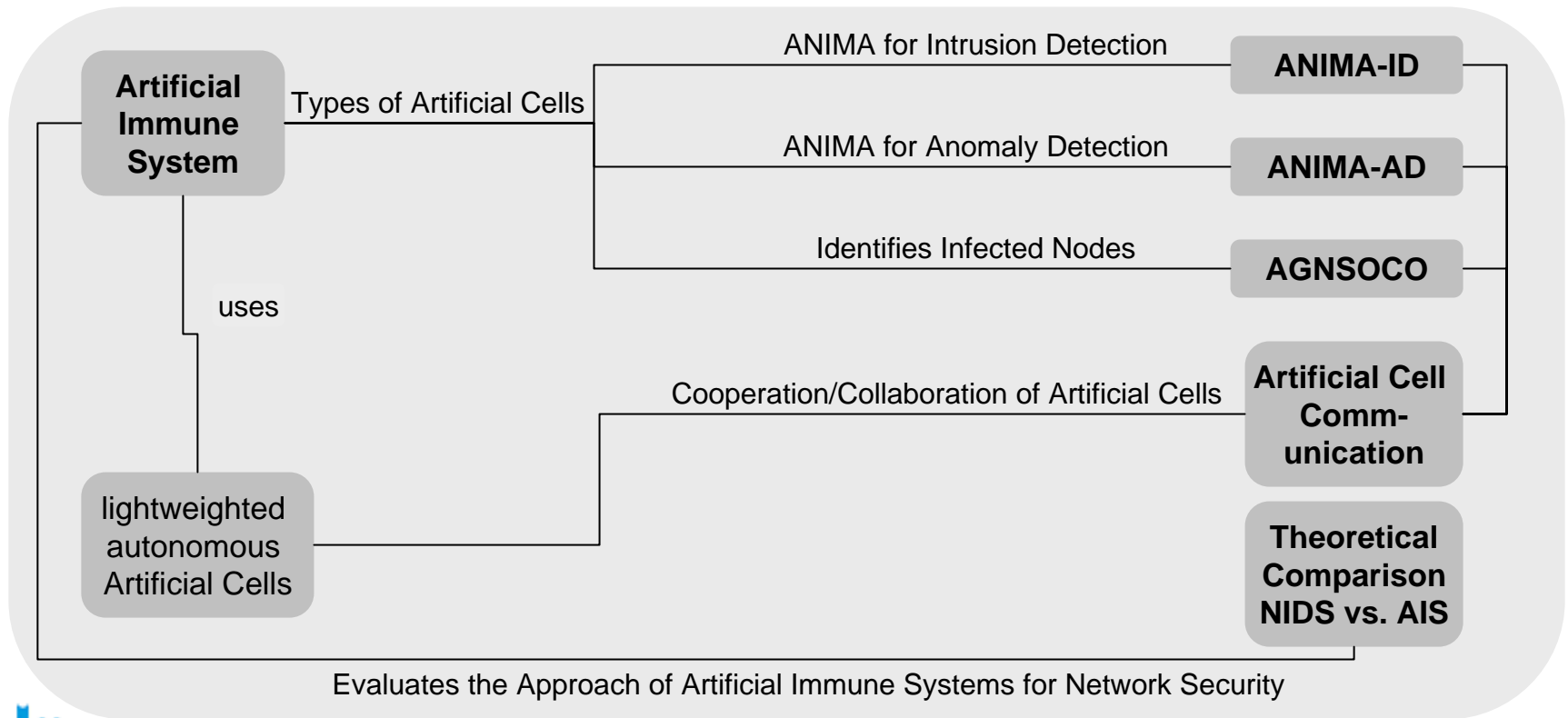
# SANA

---

- SANA – Security Analysis in Internet Traffic BFR-Project funded by the Ministry.
- Introduce novel, non-standard Approaches for Network Security
- Several Sub-Projects which describe Components/Artificial Cells of the Artificial Immune System in SANA

# SANA Overview

SANA





# SANA in Detail

---

- SANA – Artificial Immune System, implemented in Java
- Bases on a Network Simulator which simulates a Packet-Oriented Network and uses the Adversarial Queueing Theory
- An Adversarial injects Packets with and without Attacks in order to stress the Network and the Artificial Immune System.
- The artificial Cells check the Packets and remove the Packets containing an Attack. Additionally, artificial Cells perform other Tasks as well – e.g. Identification of Infected Nodes.

# SANA-AIS - Biological Inspired

- NIDS in important Nodes of the Network
  - First detection system, removes most attacks which arrive from outside – cp. the Skin of the Human Body.
- Packet Filters – Check only Packet-Header – Modeling the innate Immune System
  - Innate Immune System detects and removes basic Intrusion quickly.
- Artificial Cells – Check whole Packet and perform additional Tasks – Modeling the adaptive Immune System
  - Adaptive Immune System detects and removes complex Attacks and performs other Tasks. It also adapts to modified and novel Attacks.



# SANA Architecture

---

- Using the Implementation of SANA, it is possible to add complex Attacks and simulate complex Scenarios.
- In the SANA-AIS, it is possible to model nearly all immunological Processes.
- Currently, the Second-Signal/Co-Stimulation and a first version of Cytokines are implemented.



# SANA Scenarios

---

- Defined in a Scenario:
  - Topology of the Network
  - Behaviour of Adversarial / Artificial Cells
  - As the case maybe Topology / Behaviour of NIDS
  - Number of Time-Steps to simulate
- After the Simulation:
  - Number of founded Attacks
  - Number of finished Attacks
  - Number of False-Positives
- Currently at least 15 Simulations with different Attacks, Adversaries, Agents and Networks.



# SANA Results

---

- SANA performs well in most Scenarios.
- SANA identifies about 60% - 80% of the Attacks.
- In cooperation with a NIDS, the Network is secured against nearly all Attacks (approx. 85% - 95%).
- Furthermore, SANA adapts to the current Attack-Status:
  - Identification of modified Attacks (Mutations)
  - Immunization of a Sub-Network
  - Identification of Infected Nodes



# Next Steps

---

- Currently, there exist two different Approaches for Network Security:
  - Centralised (e.g. NIDS):  
A Server which checks each Packet routed over it. All other Nodes are not secured.
  - Distributed (e.g. AIS):  
A System which runs on each Node and all Packets on all Nodes are checked.
- In this Sub-Project, I compare the two Approaches theoretically. Therefore, I compare the two Approaches in different Models.
- However, the best Approach is a Combination of Centralised and Distributed Network Security Systems, e.g. a NIDS and SANA.



# Next Steps

---

- The Human Immune System consists of lot of Cells. These cells cooperate/collaborate in order to secure the Human Body properly.
  - Example: Minimizing False-Positives – the Body would remove itself – using cooperation between Cells and Redundancies.
- In this Sub-Project, I analyse the Cell Communication in the Human Body in order to reuse the used Techniques for SANA and for Computer Science generally.



# Say Thanks

---

- Organizers of this Workshop “Thrustworthy Software 2006”
- Supervisor of my Project, Prof. Dr. Christoph Schommer
- Ministry of Culture, higher Education and Research, Department of science and applied Research and the Fonds National de la Recherche
- Prof. Dr. Alexsander Weron from the Hugo-Steinhaus-Center, Wroclaw University of Technology, Poland
- Zdzislaw Suchanecki, Ulrich Sorger and Foued Melakessou from the INTRA-Project, University of Luxembourg
- Professors as well as PhD-Students from the University of Luxembourg



# Conclusion

---

- Network Security is an important and interesting Field of Computer Science
- The Number of Attacks decreases. However, the Attacks are more intelligent and complex.
- Existing NIDS cannot deal with this attacks.
- Hence, novel Approaches for Network Security are necessary. One example is the artificial Immune System.
- SANA is a Prototype of an artificial Immune System and consists of novel, non-standard Approaches for Network Security.



# Publications

---

- M. Hilker, C. Schommer: AGNOSCO – Identification of Infected Nodes with artificial Ant Colonies. Proceedings of the 6<sup>th</sup> International Conference on Recent Advances in Soft Computing (RASC2006) July 2006, Canterbury, United Kingdom (to appear).
- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop (AISW-NetSec 2006) during the Australasian Computer Science Week January 2006, Australia, Hobart. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54.
- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005 December 2005, Slovenia, Bled.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis at the JW Goethe-University Frankfurt, Germany, March 2005.