



SANA – Security Analysis in Internet Traffic

Michael Hilker

University of Luxembourg, Campus Kirchberg

Dept. of Computer Science and Communication

6, Rue Richard Coudenhove-Kalergi, L-1359 Luxembourg

e-mail: michael.hilker@uni.lu, phone: +352-091-886537



Agenda

- Topics of Research
- Current Situation
 - Literature
 - My Research: SANA and Subprojects
- Scientific Goal
- Publications
- Work Plans
- Extending the Project
- Conclusion



Topics of Research

- Abstract:
Secure a Network against Attacks/Intrusions
- NIDS (Network Intrusion Detection Systems)
- Intrusion / Anomaly Detection
- Ant Colonies, Artificial (Immune) Systems,
Biological Inspired Systems



Current Situation

- Networks are under a constant Assault from Intrusions, e.g. Viruses, Worms, Trojans.
- Network Intrusion Detection Systems: SNORT
 - Centralised, Semi-Automatic and Local Systems
 - Need plenty of Computational Power
- Existing Artificial Immune Systems are either
 - Autonomous or Centralised



SANA

- My Project: **SANA**
Security Analysis in Internet Traffic
- Artificial Immune System which secures the Network (Artificial Body) with autonomous, light-weighted Agents (Artificial T-Cells) against Intrusions (Artificial Pathogens).
- Agents simulate the behaviour of all cells of the Immune System, especially the T-/B-Cells.



Architectural Overview SANA

- The main Component of SANA is the Agent. The Idea of an Agent is to model the behaviour of T- and B-Cells containing to the Human Immune System.
- An Agent flows through the Network, stays for some time in a Network-Node, checks each Packet and evaluates whether the Packet is good or bad. It knows how to proceed with Bad-Packets as well.
- Each Agent works autonomous without a central system. However, agents have the possibility to cooperate.
- Using the Agent and other Components, it is possible to model nearly all immunological Processes in SANA.

Advantages and Disadvantage of SANA

- Advantages:
 - Distributed, secures the whole Network
 - Computational Power is shared over the Network
 - Adaptive, learns how to detect new Attacks
 - Autonomous, works without central Center
 - Cooperation between Agents as well as other SANAs
- Disadvantage:
 - It is not guaranteed that an important Computer is secured against all known Attacks (fixable using a NIDS in this Computer)



Subproject: ANIMA for ID

- ID (Intrusion Detection):
Store the Information how to identify Intrusions.
(similar to the Work Flow of a Virus-Guard)
- Using ANIMA in order to store the Information in a directed Graph and check each Packet against these Graph. The System returns whether the packet is good, bad or bad with high probability.
- The Approach is adaptive, autonomous and saves Storage as well as System Time.



Subproject: ANIMA for AD

- AD (Anomaly Detection):
Store the Information how to identify normal Network-Traffic. Consequently, the other Traffic is abnormal and contains Intrusions.
- I used ANIMA to store the Information of normal Traffic in an undirected Graph. The system checks each Packet against the stored Information in order to evaluate if the Traffic is normal or abnormal.
- The system is adaptive, efficient as well as autonomous. It learns autonomous how to identify novel normal Traffic and thus it adapts to the current Network-Traffic.



Subproject: Ant Colonies

- Ant Colonies:
Ant moves through the Environment and releases Pheromones which help the Ants to navigate and to find Preys.
If an Ant carries a Prey it releases a lot of Pheromones and else only some Pheromones.
- I have the Vision to use this idea for the Identification of infected Nodes.
All Packets behave like an Ant without Prey except the Confirmation-Packets for a Bad-Packet behaves like an Ant with Prey.
The Pheromones point to the Infected Node and maybe it is possible to design an Agent which identifies infected Nodes.



Project Status

- A first Prototype of SANA is implemented based on a Network Simulator.
- I tested the Prototype using several Scenarios of Attacks. In these Simulations, SANA identifies about 80-85% of the Attacks.
- First Immunological Processes for Attack and Defence are included. In detail, the Second Signal is implemented in SANA.
- ANIMA-ID is analysed, implemented and simulated. The Results will be presented in a Workshop during a Conference-Week in Hobart, Australia.
- ANIMA-AD is analysed, implemented and I currently simulate the approach. There exist currently no interesting Results.



Scientific Goal

- A Solution for the Problem of Network-Security against Intrusions. Hence, it should be an overall Solution for Network-Security.
- The Solution should provide a good Security-Level using low Administrative-Power. It also should share the needed Computational Power over all Network Nodes.
- Furthermore, SANA should contain several novel and up-to-date Approaches in Intrusion as well as Anomaly Detection.



Publications

- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop (AISW-NetSec 2006) January 2006, Australia, Hobart. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54. To be published.
- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005 December 2005, Slovenia, Bled Lake. To be published.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis at the JW Goethe-University Frankfurt, Germany, March 2005.



Short-Term Work Plan

- Short-Term Work Plan for the next Weeks:
 - Enhance SANA with an improved Visualisation. (Cooperation with TFE-Student Oltjon Sulanjaku)
 - Simulate ANIMA-AD in order to verify the Approach as well as to find appropriate Values for the Parameters.
 - Analyse the Idea of Ant Colonies for Network Security, maybe implement it as well as simulate it based on SANA.



Long-Term Work Plan/Outline

- Introduce a novel Intrusion-Model and implement it in SANA. With this, build up an Interface for an easy Attack as well as Scenario Creation-Tool.
- Enhance SANA using immunological Processes in Attack as well as Defense.
- Further on in fundamental Research for Network Security, Intrusion/Anomaly-Detection as well as Artificial Immune Systems.

Extending the Project Student Projects



- Introduce an Intrusion Model in order to describe the world of Attacks. Furthermore, use this model for Implementing an easy-to-use Scenario-Creation-Tool.
- Thinking about a Feedback-Center for Agents in order to validate past Decisions about Packets. With this, it is possible to implement Agents which perform a learning.
- Creating several Scenarios in order to use more immunological Processes as well as to test SANA.
- Migrate SANA from the Implementation based on a Network-Simulator to an Implementation which is distributed over a lot of Network-Nodes. (Simulating in real Network-Conditions)



Conclusion

- Network Security and Intrusion Detection is still a real Problem.
- SANA is an artificial Immune System in order to protect a Network.
- Some novel Approaches for Intrusion as well as Anomaly Detection
- The Outlook of my PhD is to Implement a Solution for Network Security.