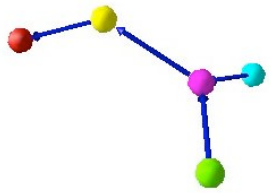
UNIVERSITÉ DU LUXEMBOURG



SANA - Network Protection through artificial Immunity

Michael Hilker & Christoph Schommer

University of Luxembourg
Faculty of Science, Technology, and Communications
6, Rue Richard Coudenhove-Kalergi
1359 Luxembourg

email: {michael.hilker, christoph.schommer}@uni.lu

http://mine.uni.lu

Protection System

- Protects a network against intrusions
- Intrusions are e.g. viruses, worms, trojans, and hackers
- Intrusions are defined as all attacks towards a network, i.e. also intrusive behaviour from users
- Facilitates, organizes, and connects different protection components

Protection Components

Host-based:

- Antivirus Software
- Firewall
- Intrusion Prevention System (IPS)
- Spam Filter

Network-based:

- Packet Filter
- Intrusion Detection System (IDS)
- Spam Filter

Current Situation

Current Situation

- A static collection of unconnected protection components is used:

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall
  - Network-based: packet filter and IDS

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall
  - Network-based: packet filter and IDS
- Protection Components work supervised

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall
  - Network-based: packet filter and IDS
- Protection Components work supervised
  - lots of warnings and alerts

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall
  - Network-based: packet filter and IDS
- Protection Components work supervised
  - lots of warnings and alerts
  - time-intensive maintenance workflows

Current Situation

- A static collection of unconnected protection components is used:
  - Host-based: antivirus software and firewall
  - Network-based: packet filter and IDS
- Protection Components work supervised
  - lots of warnings and alerts
  - time-intensive maintenance workflows
- No collaborative work in order to find mutated or even novel intrusions

SANA approach

- Distributed approach with redundant installed infrastructure
- Elimination of single points of failures
- Easy and fast maintenance workflows, i.e. administration, update, extension
- Use a better organization with cooperation in order to cope with upcoming intrusions

SANA approach

SANA approach

SANA approach

Protects all nodes

SANA approach

Protects all nodes

Easy Updateable
and Expandable

SANA approach

Protects all nodes

Easy Updateable
and Expandable

Cooperative

SANA approach

Protects all nodes

Easy Updateable
and Expandable

Self-Organized

Cooperative

SANA approach

Protects all nodes

Autonomous Workflows

Easy Updateable and Expandable

Self-Organized

Cooperative

SANA approach

Protects all nodes

Autonomous
Workflows

Easy Updateable
and Expandable

Self-Organized

Cooperative

Adaptive
Self-Learning

SANA approach

Protects all nodes

Autonomous
Workflows

Easy Updateable
and Expandable

Self-Organized

Cooperative

Adaptive
Self-Learning

Self-Checking

SANA approach

Protects all nodes

Autonomous
Workflows

Easy Updateable
and Expandable

Self-Organized

Cooperative

Adaptive
Self-Learning

Self-Repairing
Self-Healing

Self-Checking

SANA approach

Migration task:

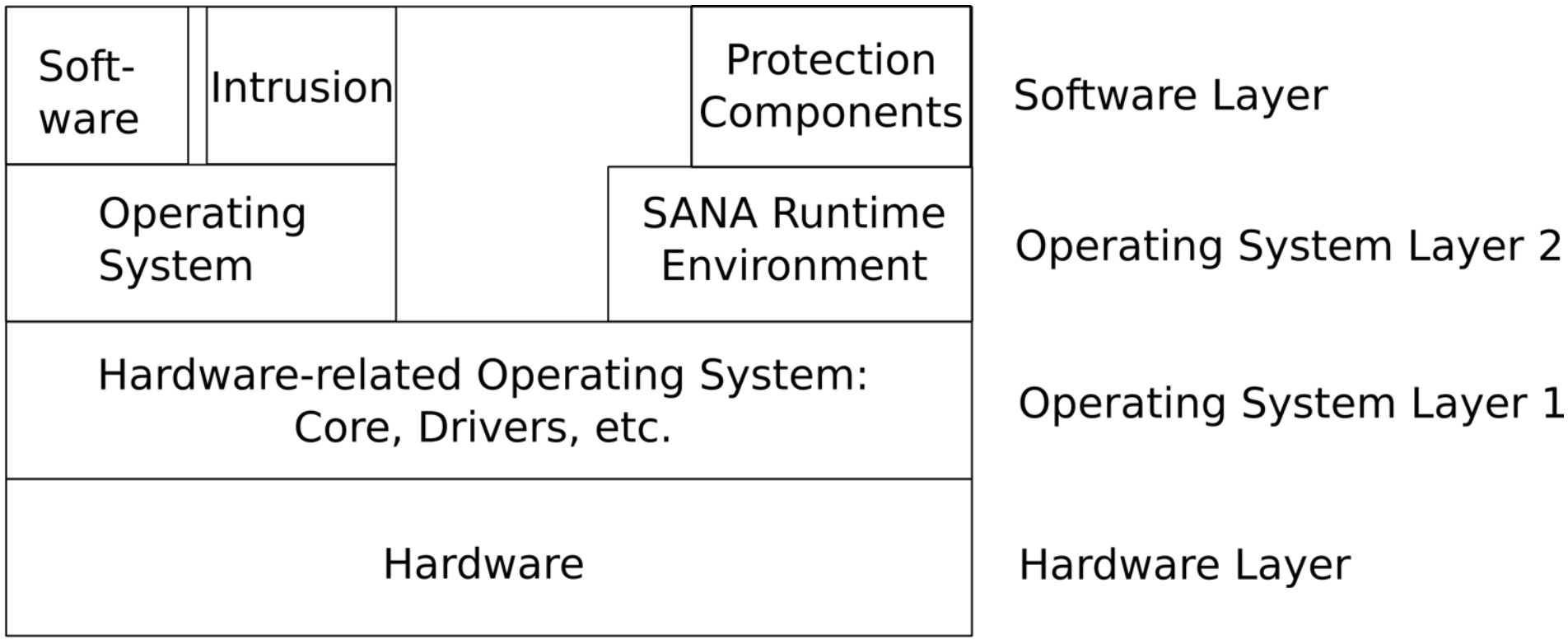
- Currently:
  client-server architecture; server manages the client software performing the required tasks

- Goal:
  - distributed architecture with autonomous artificial cells performing the required tasks and enable additional features

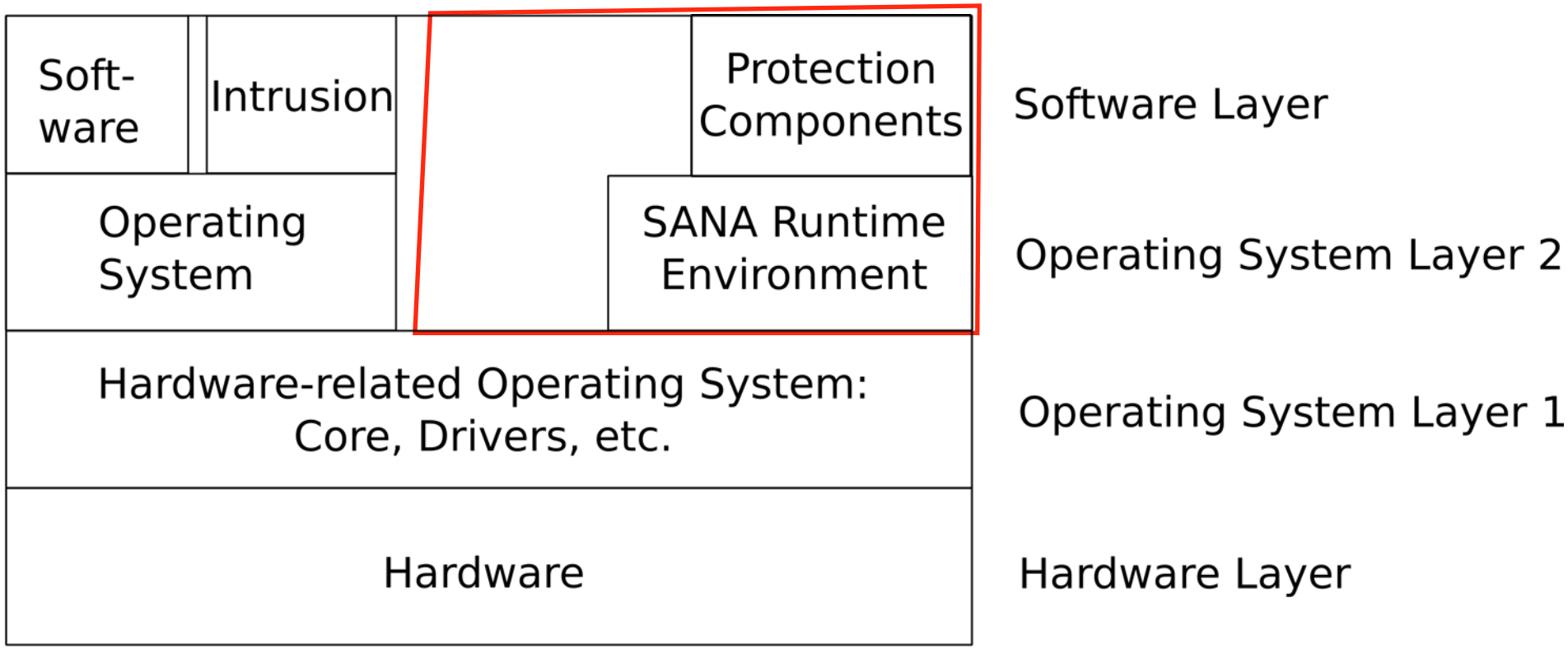
Security Environment

- Installed in each node as a middleware between protection components and resources
- All protection components run in this environment
  - Protection components are platform independent, which leads to a faster implementation

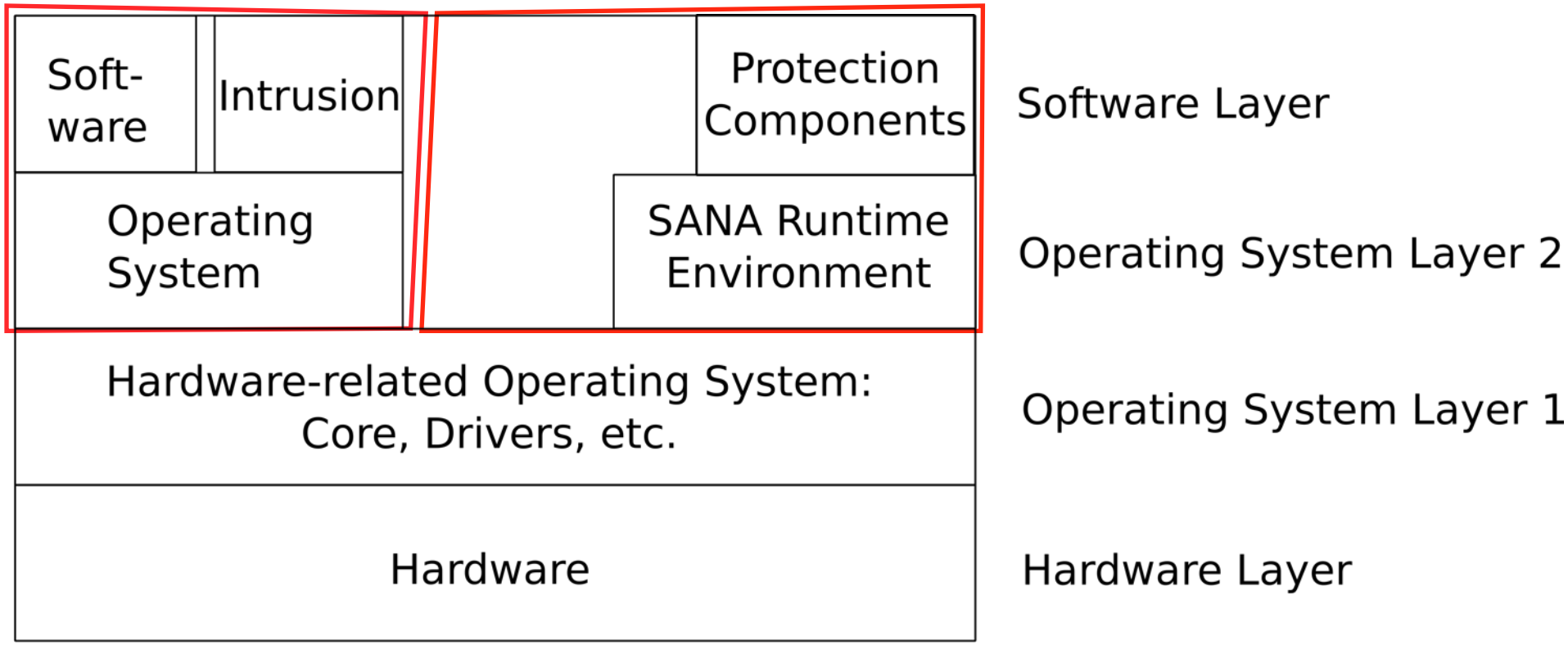
Implementation Security Environment



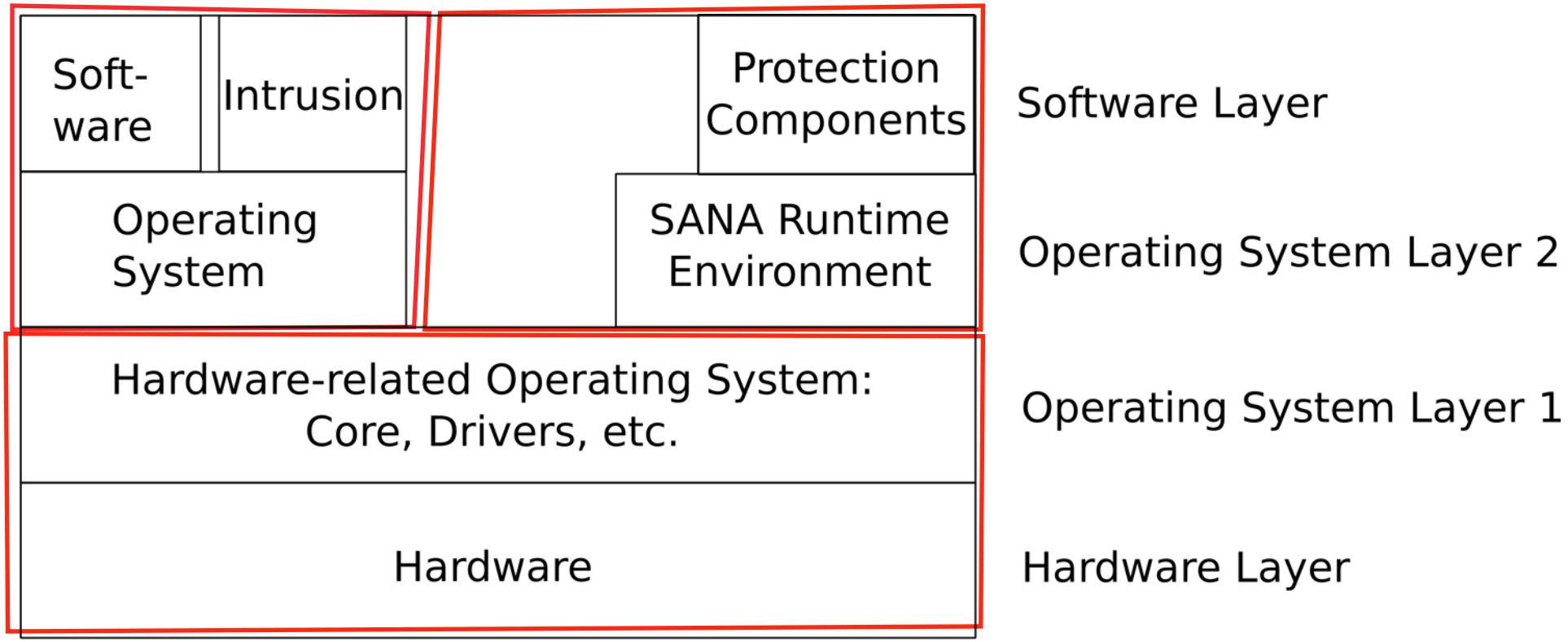
Implementation Security Environment



Implementation Security Environment



Implementation Security Environment



Artificial Cells

- Novel type of protection components performing certain tasks for network security
- Tasks are e.g.
  - packet/file/process checking
  - identification of infected nodes or not proper working components
  - performing regular checks
  - information as well as data collecting
- Artificial cells (Agents) move through the network in order to provide a highly dynamic protection system

Examples of artificial Cells

Examples of artificial Cells

- ANIMA for Intrusion Detection
  Uses a network-like structure in order to store signatures of intrusions. Analyses and evaluates network packets.

Examples of artificial Cells

- ANIMA for Intrusion Detection
  Uses a network-like structure in order to store signatures of intrusions. Analyses and evaluates network packets.
- AGNOSCO
  Reuses the information gathered through distributed network traffic analysis for the identification of infected nodes, which is motivated by artificial ant colonies.

Examples of artificial Cells

- ANIMA for Intrusion Detection
  Uses a network-like structure in order to store signatures of intrusions. Analyses and evaluates network packets.
- AGNOSCO
  Reuses the information gathered through distributed network traffic analysis for the identification of infected nodes, which is motivated by artificial ant colonies.
- Checking Cells
  Perform regular checks in order to identify infected nodes, not proper working and outdated components, and even abnormal behavior - implementation of self-checking.

Examples
Checking Cell

Examples
Checking Cell

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
toor:x:0:0:root:/root:/bin/bash
```

Examples
Checking Cell

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
toor:x:0:0:root:/root:/bin/bash
```

Characteristics of known intrusions:

- Existing files
- Running processes
- Registry entries

E.g. Bagle:

- File bbeagle.exe in system-dir
- Process bbeagle.exe running
- Registry:
  - [HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d3dupdate.exe]
  - [HKCU\Software\Windows98\frun]
- Email propagation

Artificial Lymph Nodes

- Supply on demand the artificial cells with additional information and resources
- Response to messages sent by the artificial cells
- Manage the communication between the different cells
- Redundant installed so that a breakdown is compensated by other artificial lymph nodes and that the distance from cell to lymph node is short
- Collect status information about the supplied network part

Central Nativity and Training Stations

- Motivated by the bone marrow and thymus
- Generate and release continuously novel artificial cells containing the newest information and approaches of network security where existing artificial cells shutdown over time
- Supply the artificial lymph nodes with additional information and resources
- Collect status information, which are on demand sent to the administrators

Artificial Cell Communication

- Robust and efficient communication protocol for exchanging messages between a sender a set of receivers - point to multi-point communication
- Uses no communication server
- Efficient when a message is sent in a small area; e.g. notifying nearby artificial cells about a certain event
- Adapts so that a partly breakdown does not implicit a breakdown of the whole communication in the network
- Artificial receptors (public/private key pair) identify the receivers of a message

Self-Management

- Organizes the artificial cells so that each node has enough but not too much cells
- Manages the cells so that regular checks are done on all nodes but not too often on one node
- Adapts the system to the current situation and protects important nodes with a higher security

Collaborative Work

- Splitting of workflows in small tasks:
  - Information collection
  - Information evaluation
  - Response
- Second signal:
  two components have to evaluate a packet
  as malicious so that it is removed

Collaborative Work Danger Theory

- Information sharing between different security components, which are mostly nearby
- Each cell releases to the neighbors summary status information - the signals - about its current view of the situation
- Use the information in order to adapt the internal thresholds and the organization of the protection components
- Collect important information for reporting to the administrator

Adaptive System

- SANA identifies infected nodes:
  - Disinfection
  - Isolation
- SANA recognizes hotspots of attacks and adapts with a higher concentration of cells
- Self-checking and afterwards self-repairing/-healing
- Internal adaption on current situation - danger theory

Maintenance Workflow

- Administrators demand regularly information from the security system
- Administrators also configure the system
- Through a GUI-interface, the administrators can connect to the security environments of all nodes. In the environment, the administrators can access the protection components.
- Artificial lymph nodes and CNTS collect status information, which can be demanded by the administrators
- Important information (e.g. alerts) are immediately sent to the administrators

Maintenance Workflows Updates & Extensions

- Artificial cells are renewed over time including the newest information
- Other security components are updated using two workflows

    1. Updating artificial cells

    2. Direct installation into the security environment by the administrator

- Extensions are released through a new population of artificial cells or direct connection to the security environment

Simulations

- System is implemented on top of a network simulator implementing a packet-oriented network (TCP/IP)
- Different attack-scenarios are implemented, e.g. worm and virus attacks
- Various other attack-scenarios like hacker attacks are theoretically discussed

Results

- SANA's performance is more than acceptable
- SANA facilitates the same protection components as common used protection systems supplemented with the novel artificial cells

% of identified infected packets	Current Security System	SANA
Worm Attack	75% - 85%	95% - 99,9%
Virus Attack	60%	78%-85%

Results

- The behavior of SANA is dynamic and adaptive
- Hard-to-attack through the distributed architecture, reduced single points of failures, and autonomous workflows
- SANA provides a framework that can be quickly extended by novel approaches of network security

Results

- SANA identifies quickly infected nodes and not proper working/outdated components
- Infected nodes are either disinfected or quarantined and then disinfected by the administrator
- Abnormal behavior is identified through analyzing information from various nodes with different techniques
- Tasks are distributed so that a partly breakdown does not implicit a complete breakdown of the system

Attack Scenario
Worm Attack

- Uses the network for propagation
- Infects a node, influences the production, and sends infected packets in order to infect other nodes
- SANA identifies the infected packets and prevents the propagation
- SANA identifies the infected nodes and disinfects these
- Adapts the workflows to prevent attacks
- After some time, SANA disinfects and immunizes the network

Attack Scenario
Virus Attack

- Arrives at the node without usage of the network
- Infects the node and propagates to other nodes using data transmission
- SANA identifies the infection using regular checks and the detection of infected packets
- SANA isolates and disinfects the node
- Immunization through updating the security components

Attack Scenario Hacker Attack

- Attacks the node directly over the network, with physical access, etc.
- Installs mostly a backdoor (e.g. VPN-server with IPsec) for further attacks
- Uses the infected node to access resources all over the network
- SANA identifies the backdoor using regular checks and traffic analysis
- Observing of access to resources identifies not allowed access and inference to node and user
- Closing of backdoor and immunization

Resource Management

- Tasks are distributed over all nodes
  - Resource need on a single node is reduced
- Efficient implementation of the security environment reduces required resources
- Self-management reduces redundant tasks and thus also reduces the required resources

Conclusion

Conclusion

Artificial Immune System

Conclusion

Artificial Immune System

Security Environment

Conclusion

Artificial Immune System

Security Environment

Artificial Cells

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Conclusion

Artificial Immune System

Security Environment

Self Management

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Conclusion

Artificial Immune System

Security Environment

Self Management

Artificial Cell Communication

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Conclusion

Artificial Immune System

Security Environment

Self Management

Artificial Cell Communication

Artificial Cells Protection Components

Collaborative Work

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Self Management

Artificial Cell Communication

Collaborative Work

Self Checking

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Self Management

Artificial Cell Communication

Collaborative Work

Self Checking

Self Healing / -Repairing

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Self Management

Artificial Cell Communication

Collaborative Work

Self Checking

Self Healing / -Repairing

Dynamic System

Conclusion

Artificial Immune System

Security Environment

Artificial Cells Protection Components

Infrastructure:
Artificial Lymph Nodes
Central Nativity and Training Stations

Self Management

Artificial Cell Communication

Collaborative Work

Self Checking

Self Healing / -Repairing

Dynamic System

Adaptive System

Conclusion

- SANA is a framework to implement a distributed security system. It provides a library of non-standard approaches for protection components combined with common-used components. The organisation and the information management is more sophisticated for lots of collaboration between the components.
- Middleware for security components
- Artificial cells - small components - collaborating for the performance of the overall system

Next Steps

- Discussion how to implement the security environment so that adversaries cannot use the security system for attacks
- What are the challenges in bringing an artificial immune system for network security from an academic research to a productive status?
- Danger Model - continous exchange of status information in order to adapt the internal thresholds

Acknowledgments

- Organizers of TCV 2007, esp. Jean-Yves Marion, Eric Filiol, Guillaume Bonfante
- FSTC, ILIAS, and INTRA
- Fonds National de la Recherche
- Ministère de la Culture de l'Enseignement Supérieur et de la Recherché

References

2007

- B. Schroeder, M. Hilker, R. Weires: Dynamic Association Networks in Information Management. Proceedings of the 4th International Conference on Machine Learning and Data Analysis (MLDA 2007), May 2007, Vienna, Austria. (to appear)
- M. Hilker, C. Schommer: SANA - Network Protection through artificial Immunity. Proceedings of the 2nd International Workshop on Theory of Computer Viruses (TCV 2007), May 2007, Nancy, France. (to appear)
- C. Brucks, C. Wagner, M. Hilker, R. Weires: CoZo - Content Zoning for Spam Emails. Proceedings of the 3rd International Conference on Web Information Systems and Technologies (Webist2007), March 2007, Barcelona, Spain.

2006

- M. Hilker, C. Schommer: AGNOSCO – Identification of Infected Nodes with artificial Ant Colonies. Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC2006), July 2006, Canterbury, United Kingdom.
- M. Hilker, C. Schommer: SANA - Security Analysis in Internet Traffic through Artificial Immune Systems. Proceedings of the Trustworthy Software Workshop 2006, May 2006, Saarbruecken, Germany.
- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop - Network Security (AISW-NetSec 2006). Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54. January 2006, Hobart, Australia.

2005

- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005, December 2005, Bled, Slovenia.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis, Johann Wolfgang Goethe-University, March 2005, Frankfurt, Germany.