

Service Oriented Architecture in Network Security

-

a novel Organisation in Security Systems

Michael Hilker
University of Luxembourg

michael.hilker@gmail.com
+352-466644-5415

Research Layers

- Detector Generation
- Detector Organisation
- Results/Response Management

Service Oriented Architecture

- Novel paradigm to see everything as a service
- Services are provided on demand
- Cooperation to reuse results
- Reuse existing solutions

Virtualization

- Use a virtualization system to provide virtual machines
- Virtual machines provide the operating system with installed application
- Virtual machines can be duplicated, halted, and copied to other nodes.

Network Security

- Collection of various security components, e.g. antivirus software, firewall, IDS
- Each component is directly installed in the operating system
- Each component works on its own

Network Security Research

- Approaches to implement a real distributed integrated security system
- Many approaches aim in the direction of multi-agent system or artificial immune systems
- Well, actually, how to implement such a system?

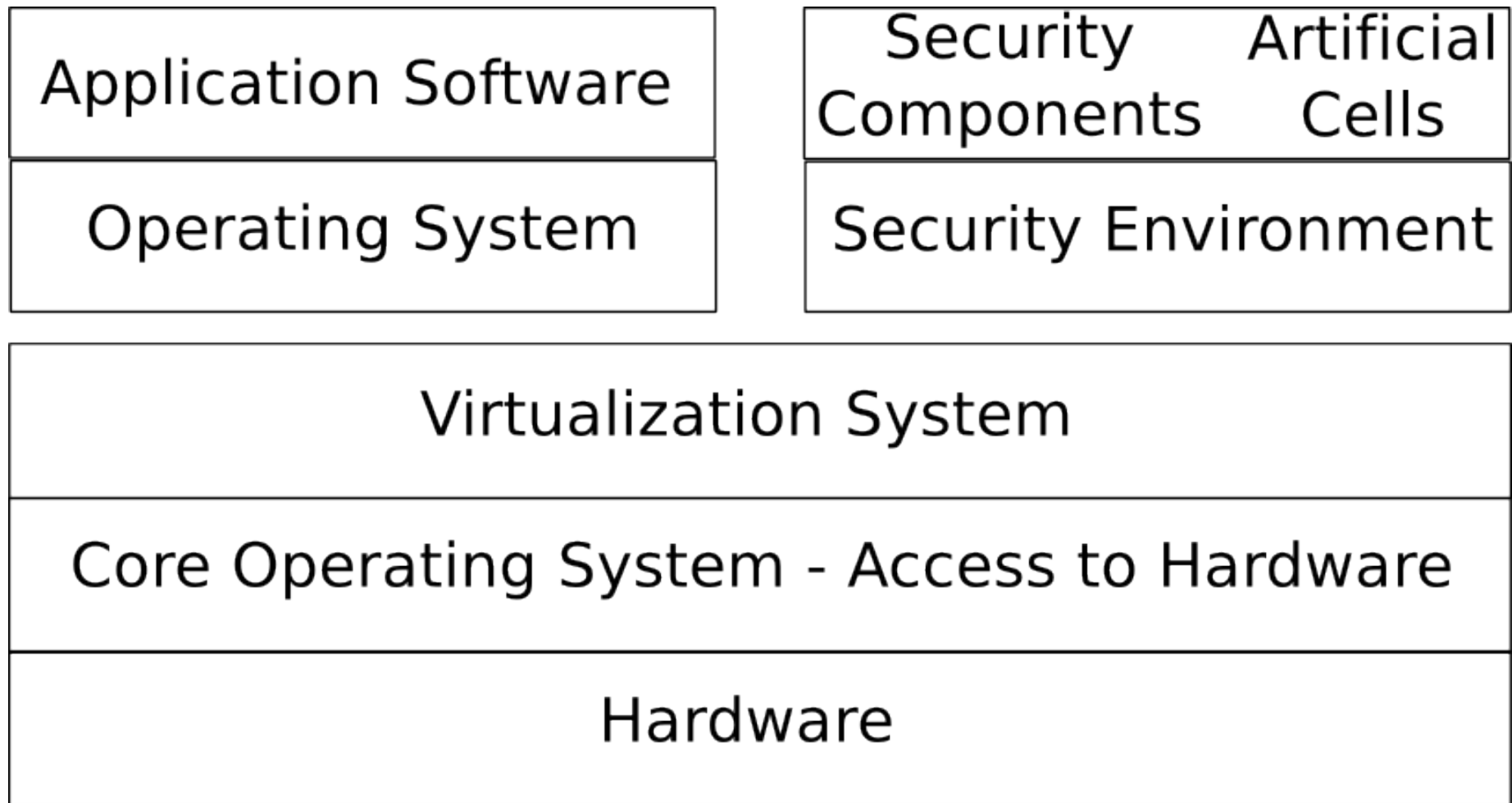
Demanded Features of novel System

- Easy maintenance
- Quickly extendable
- Copes with upcoming intrusions
- Protects all types of nodes in a network (i.e. novel nodes as thin clients and mobile phones are a challenge)

Proposed Architecture

- Nodes are fully virtualized
- Security components run in a different virtual machine than the operating system
-> checking from outside
- Security components are on demand provided by a security server
- Infected virtual machines are disinfected, copied and analysed for further steps

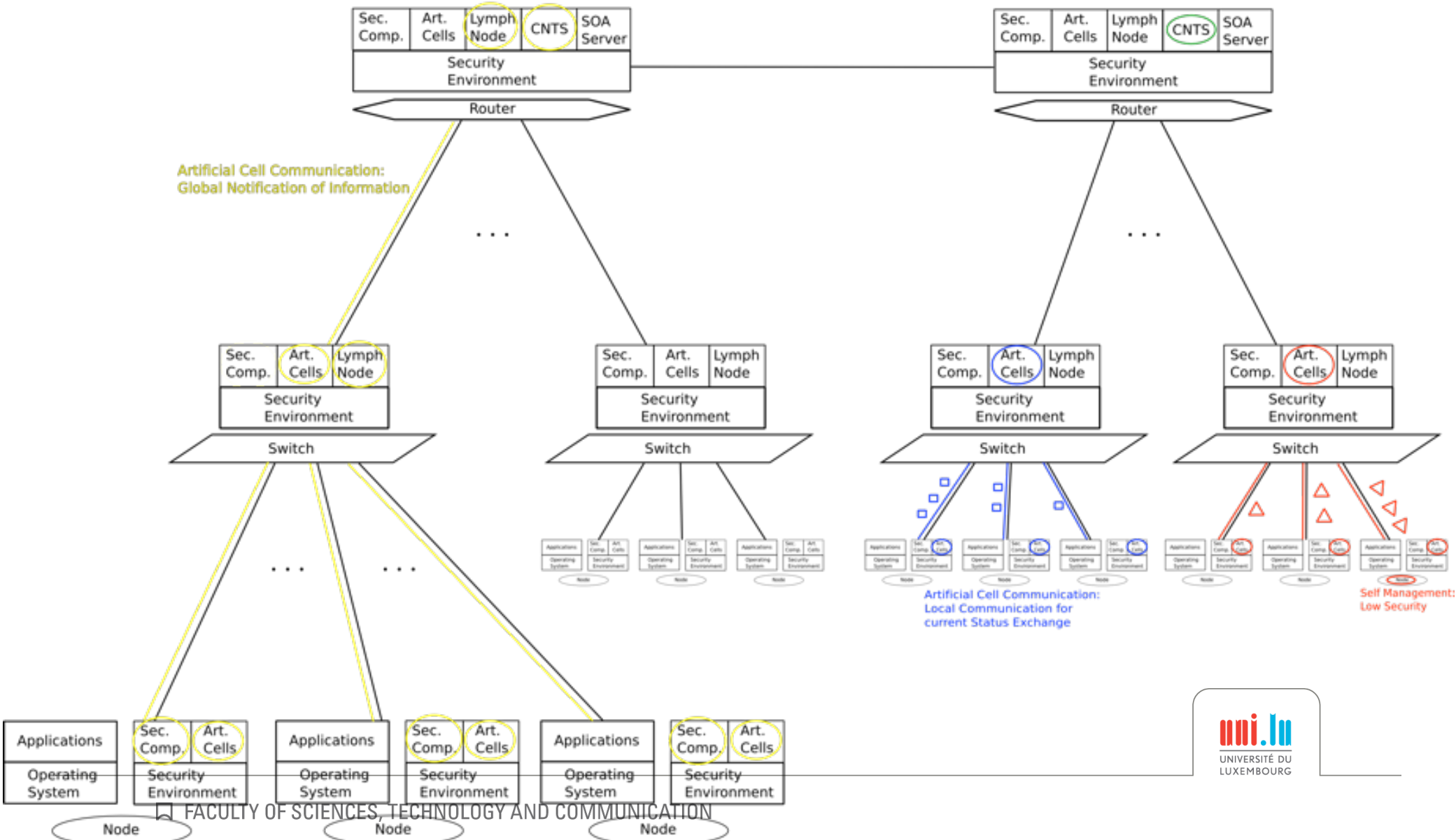
Node Architecture



Network Architecture

Generation of new Cells

Artificial Cell Communication: Global Notification of Information



Maintenance

- When a node connects to the system, after infection, or after some time, the node's security is checked
- The neighbours use integrity checks to identify changes in the security system
- Unsecured nodes are disconnected to prevent intrusion propagation

Infection Handling

- A virtual machine of a node is infected:
 - It is halted to prevent propagation
 - It is copied to the security server for analysis and legal aspects
 - A clean virtual machine is demanded to minimise downtime
- Other parts of the architecture cannot be infected due to integrity checks

Project Status

- Research on virtualization and SOA to identify the potential
- Research on the potential of a real distributed security system
- First virtualization prototype testing the feasibility of the architecture

Future Work

- Extend prototype to a functional node implementation
- Secure implementation of a node
- Network prototype basing on an open-source virtualization system with additional required features

Application - SANA

- Distributed security system basing on the paradigm nature with sophisticated organisation of intrusion detectors
- Artificial cells encapsulate common used detection workflows and roam through the network
- Cooperation, information management, and exchange of results increase the detection performance
- Architecture with virtualization and SOA is the basis for implementing this system

Conclusion

- Novel architecture enables several additional features
- Implementation with virtualization and SOA is feasible
- Copes better with upcoming intrusions

Thanks for your attention