Securing BIONETS:
"How can Security Infrastructures Match Autonomically Evolving Networks and Services?"

Daniel Schreckling
Security in Distributed Systems (SVS)
http://www.informatik.uni-hamburg.de/SVS/
University of Hamburg

DISTTRUST Workshop
Barcelona, April 28, 2006
Outline

BIONETS
- Motivation
- Goals
- Approach

Security in BIONETS
- Traditional Security Assumptions
- Assumptions in BIONETS
- The Challenge

Services in BIONETS as an Example
- Securing a Highly Dynamic Framework
- A Vision: Evolution of Security Services
BIOlogically-inspired autonomic NETworks and Services

Motivation

- Pervasive Computing and Communication Environments
- Deficiencies of Existing Communication Approaches
- Systems in Nature and Society with Large Populations able to
  - Develop Collaboration and Survival Strategies
  - Work in Absence of Central Control
  - Exploit Local Interaction

Main Goals

- Complement and Improve Current Networking Infrastructures
- Support Local Networks with Large Number of Heterogeneous Devices
- Design Services able to Adapt to the Environment
- Provide Situated and Autonomic Communications
The BIONETS Paradigm

Two-Tier architecture
- T-Nodes (Tiny devices, Limited Resources, Minimum Functionality)
- U-Nodes (Rich Network/Service Functionalities)

Strong Locality
- Peer-to-Peer Communication
- One Hop Communication
- “Disappearing Network”
- Service/User Centric Approach

Biologically-Inspired
- Self-Managed Services
- Services Adapting to the Environment
- Service Evolution to Satisfy User Needs

BIONETS Security: The Big Picture

Security Needs to Build upon Something Static, e.g.:
- Public-Key-Infrastructures
- Communication Links between Principals
- Security Modules

BIONETS Aim at the Opposite:
- Ad-Hoc Networking
- One Hop Communication
- Information Restricted in Time and Space
- No Network Management but Self-Configuration
- Service Evolution

The Challenge for Security:
- How Far can we Push Security Technology to Meet These Goals?
- Find the “Least Securable Architecture”: What are the Minimal Assumptions for BIONETS we can Deal with?
Example: Services in BIONETS

BIONETS are Centred Around Services

- Security Itself is Seen as a Service
- Security Needs to Consider Other Services as Principals
- Communication-Level Security Between Nodes is not Enough

Characteristics of Services in BIONETS

- New Services can be Created through Local Combination
  - Is it still Possible to Comply with Security Requirements?
- A Service may be Distributed among Several Nodes
  - What is/are the Principals and how to Secure them?
- Services Require to be Monitored
  - Can we do this Reliably in a Distributed and Disconnected Environment?
Services in BIONETS: There is more ...

BIONETS Provides Service Evolution

- Principals Change, Disappear, or are Being Created
  - How Can we Cope with this?
- Evolving Services can have (Previously Unknown) Security Requirements
  - Can we Form Security Services that Match new Requirements?

The Vision: Evolving Security

- Since Security is Seen as a Service, it should Also Evolve
  - What could be Suitable Parameters?
  - How would a feasible Fitness Function Look Like?
  - What are the Security Primitives which should not Evolve?
Summary

Main Focus is not on how to Secure Communication but on:

How Security Infrastructures can Match Evolving Networks and Services!

"the architect of the future will build inspired by nature because it is the most rational, the most durable, and the most economic of all methods."

Juan Torres (1810)
http://www.bionets.org/

Thank you for your Attention!

For more information on Security in BIONETS
schreckling at informatik dot uni-hamburg dot de