Security in BIOlogically-inspired Networks and Services

Daniel Schreckling

Security in Distributed Systems
University of Hamburg
schreckling at informatik dot uni-hamburg dot de

September 20-21, 2006
BIOlogically-inspired NETworks and Services

http://www.bionets.eu/

Project Reference   FP6-027748
Area                  Situated and Autonomic Communications
EU Contribution      5,05 MEUR
Starting Date        2006-01-01
Duration              48 Months
Co-ordinator         Prof. Imrich Chlamtac
                      CREATE-NET (Trento, Italy)
Outline

1. BIONETS
   - Motivation and Goals
   - BIONETS Approach

2. Security in BIONETS
   - Challenges
   - Service Security

3. Research Efforts
   - Research Directions
   - Security Architecture
   - Security Policies
   - The BIONETS Ether?

4. Summary
1. BIONETS
   - Motivation and Goals
   - BIONETS Approach

2. Security in BIONETS
   - Challenges
   - Service Security

3. Research Efforts
   - Research Directions
   - Security Architecture
   - Security Policies
   - The BIONETS Ether?

4. Summary
Motivation

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

Goals

- Complement and Improve Current Networking Infrastructures
- Support Local Networks with numerous Heterogeneous Devices
- Design Services Able to Adapt to the Environment
- Provide Situated and Autonomic Communications
Motivation

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

Goals

- Complement and Improve Current Networking Infrastructures
- Support Local Networks with numerous Heterogeneous Devices
- Design Services Able to Adapt to the Environment
- Provide Situated and Autonomic Communications
BIONETS Approach

- **Two-Tier Architecture**
  - **Tiny Nodes**, Minimum Functionalities
  - **User Nodes**, Rich Functionalities (Access Point Nodes)

- **Strong Locality**
  - "Disappearing Network"
  - Service/User Centric Approach
  - Peer-to-Peer Communication
  - One Hop Communication

- **Biologically-Inspired Services**
  - Self-Managed
  - Adapting to the Environment
  - Evolution to Satisfy User Needs
BIONETS Approach

- Two-Tier Architecture
  - Tiny Nodes, Minimum Functionalities
  - User Nodes, Rich Functionalities
    - (Access Point Nodes)

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

- Biologically-Inspired Services
  - Self-Managed
  - Adapting to the Environment
  - Evolution to Satisfy User Needs
Two-Tier Architecture
- **Tiny Nodes**, Minimum Functionalities
- **User Nodes**, Rich Functionalities
  
  (Access Point Nodes)

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

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

- **Two-Tier Architecture**
  - Tiny Nodes, Minimum Functionalities
  - User Nodes, Rich Functionalities
    - (Access Point Nodes)

- **Strong Locality**
  - "Disappearing Network"
  - Service/User Centric Approach
  - Peer-to-Peer Communication
  - One Hop Communication

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

1. BIONETS
   - Motivation and Goals
   - BIONETS Approach

2. Security in BIONETS
   - Challenges
   - Service Security

3. Research Efforts
   - Research Directions
   - Security Architecture
   - Security Policies
   - The BIONETS Ether?

4. Summary
Challenges for Security

Classic Security Builds upon Static Entities
- Public-Key-Infrastructures
- Communication Links between Principals
- Security Modules (possibly signed)

BIONETS Aims at
- Ad-Hoc Networking
- One Hop Communication
- Heterogeneity
- No Network Management but Self-Configuration
- Service Evolution

Primary Challenges
- Find out how far Security Technology can be Pushed to Meet these Goals!
- Find Minimal Assumptions for BIONETS we can Deal With!
Challenges for Security

- Classic Security Builds upon Static Entities
  - Public-Key-Infrastructures
  - Communication Links between Principals
  - Security Modules (possibly signed)

- BIONETS Aims at
  - Ad-Hoc Networking
  - One Hop Communication
  - Heterogeneity
  - No Network Management but Self-Configuration
  - Service Evolution

- Primary Challenges
  - Find out how far Security Technology can be Pushed to Meet these Goals!
  - Find Minimal Assumptions for BIONETS we can Deal With!
Challenges for Security

- Classic Security Builds upon Static Entities
  - Public-Key-Infrastructures
  - Communication Links between Principals
  - Security Modules (possibly signed)

- BIONETS Aims at
  - Ad-Hoc Networking
  - One Hop Communication
  - Heterogeneity
  - No Network Management but Self-Configuration
  - Service Evolution

- Primary Challenges
  - Find out how far Security Technology can be Pushed to Meet these Goals!
  - Find Minimal Assumptions for BIONETS we can Deal With!
Services in BIONETS

- **User/Service Centric**
  - Security Itself is Seen as a Service
  - Other Services have to be Considered as Principals
  - Communication-Level Security is not Enough

- **Characteristics of Services in BIONETS**
  - Services can be Created through local Combination
  - Services may be Distributed among Several Nodes
  - Services may need to be Monitored Reliably

- **BIONETS Provides Service Evolution**
  - Principals Emerge, Change, Disappear
  - Services can have New (Previously Unknown) Security Requirements
Services in BIONETS

- User/Service Centric
  - Security Itself is Seen as a Service
  - Other Services have to be Considered as Principals
  - Communication-Level Security is not Enough

- Characteristics of Services in BIONETS
  - Services can be Created through local Combination
  - Services may be Distributed among Several Nodes
  - Services may need to be Monitored Reliably

- BIONETS Provides Service Evolution
  - Principals Emerge, Change, Disappear
  - Services can have New (Previously Unknown) Security Requirements
Services in BIONETS

- User/Service Centric
  - Security Itself is Seen as a Service
  - Other Services have to be Considered as Principals
  - Communication-Level Security is not Enough

- Characteristics of Services in BIONETS
  - Services can be Created through local Combination
  - Services may be Distributed among Several Nodes
  - Services may need to be Monitored Reliably

- BIONETS Provides Service Evolution
  - Principals Emerge, Change, Disappear
  - Services can have New (Previously Unknown) Security Requirements
Outline

1. BIONETS
   - Motivation and Goals
   - BIONETS Approach

2. Security in BIONETS
   - Challenges
   - Service Security

3. Research Efforts
   - Research Directions
   - Security Architecture
   - Security Policies
   - The BIONETS Ether?

4. Summary
Research Directions

- Routing Security
- Trust and Reputation System
- Adaptive Security and Evolutionary Security
- Privacy, Anonymity, Authenticity
- Modelling and Verification
Research Directions

- Routing Security
- Trust and Reputation System
- **Adaptive Security and Evolutionary Security**
- Privacy, Anonymity, Authenticity
- Modelling and Verification
Security Architecture

- Usual Requirements (e.g. WSNs)
  - Low Energy Resources
  - Memory Restrictions
  - Low Computational Power
  - Low Radio Coverage
  - High Latencies
  - etc.

- Security Architecture of BIONETS also has to
  - Provide Security Primitives
  - Enable Secure Local and Remote Service Combination and Execution
  - Efficient and Reliable Monitoring of Nodes
  - Provide Service and Data Security Policy Enforcement

- Architecture currently Under Review
Security Architecture

- Usual Requirements (e.g. WSNs)
  - Low Energy Resources
  - Memory Restrictions
  - Low Computational Power
  - Low Radio Coverage
  - High Latencies
  - etc.

- Security Architecture of BIONETS also has to
  - Provide Security Primitives
  - Enable Secure Local and Remote Service Combination and Execution
  - Efficient and Reliable Monitoring of Nodes
  - Provide Service and Data Security Policy Enforcement

- Architecture currently Under Review
Security Architecture

- Usual Requirements (e.g. WSNs)
  - Low Energy Resources
  - Memory Restrictions
  - Low Computational Power
  - Low Radio Coverage
  - High Latencies
  - etc.

- Security Architecture of BIONETS also has to
  - Provide Security Primitives
  - Enable Secure Local and Remote Service Combination and Execution
  - Efficient and Reliable Monitoring of Nodes
  - Provide Service and Data Security Policy Enforcement

- Architecture currently Under Review
Security Policies

Existing Mechanisms
- Classical AAA is Too Coarse Grained
- Often Only Localised Focus
- Dependent on Chronological Order
- Mainly Stateless

Features Required for BIONETS
- Strong Focus on Data
- Efficient Enforcement in a Distributed Environment
- Stateful Policies
- Automatic Combination, Modification, Inference, and Verification
Existing Mechanisms
- Classical AAA is Too Coarse Grained
- Often Only Localised Focus
- Dependent on Chronological Order
- Mainly Stateless

Features Required for BIONETS
- Strong Focus on Data
- Efficient Enforcement in a Distributed Environment
- Stateful Policies
- Automatic Combination, Modification, Inference, and Verification
The BIONETS Ether?

An execution model which may fit our needs?

- **Fraglets**
  - Inspired by Molecular Biology
  - Fraglets Unify Data and Code in one Structure
  - Represent Fragments of a Distributed Computation
  - Processing and Exchange Represent Computations

- **Characteristics of Fraglets**
  - Related to Active Networking
  - Support Automatic Protocol Synthesis
  - Support Resilience
  - Dangerous because of Data/Code Unification?

- **Results**
  - Extended by Cryptographic Primitives
  - High Affinity to MultiSet Rewriting
The BIONETS Ether?

An execution model which may fit our needs?

- Fraglets
  - Inspired by Molecular Biology
  - Fraglets Unify Data and Code in one Structure
  - Represent Fragments of a Distributed Computation
  - Processing and Exchange Represent Computations

- Characteristics of Fraglets
  - Related to Active Networking
  - Support Automatic Protocol Synthesis
  - Support Resilience
  - Dangerous because of Data/Code Unification?

- Results
  - Extended by Cryptographic Primitives
  - High Affinity to MultiSet Rewriting
The BIONETS Ether?

An execution model which may fit our needs?

- **Fraglets**
  - Inspired by Molecular Biology
  - Fraglets Unify Data and Code in one Structure
  - Represent Fragments of a Distributed Computation
  - Processing and Exchange Represent Computations

- **Characteristics of Fraglets**
  - Related to Active Networking
  - Support Automatic Protocol Synthesis
  - Support Resilience
  - Dangerous because of Data/Code Unification?

- **Results**
  - Extended by Cryptographic Primitives
  - High Affinity to MultiSet Rewriting
The BIONETS Ether?

An execution model which may fit our needs?

- **Fraglets**
  - Inspired by Molecular Biology
  - Fraglets Unify Data and Code in one Structure
  - Represent Fragments of a Distributed Computation
  - Processing and Exchange Represent Computations

- **Characteristics of Fraglets**
  - Related to Active Networking
  - Support Automatic Protocol Synthesis
  - Support Resilience
  - Dangerous because of Data/Code Unification?

- **Results**
  - Extended by Cryptographic Primitives
  - High Affinity to MultiSet Rewriting
Outline

1. BIONETS
   - Motivation and Goals
   - BIONETS Approach

2. Security in BIONETS
   - Challenges
   - Service Security

3. Research Efforts
   - Research Directions
   - Security Architecture
   - Security Policies
   - The BIONETS Ether?

4. Summary
Summary

Setting
- Large Number of Heterogenous Devices
- Service and User Centric "Disappearing Network"
- Biologically-Inspired Services
- Self-Managed, Evolving Services to Satisfy User-Needs
- Autonomic Adaptation to Environment

Focus
- Securing Communication is not Enough
- Match Security Infrastructures to Evolving Networks and Services!

Many Interesting Problems to be Tackled
Summary

Setting
- Large Number of Heterogenous Devices
- Service and User Centric "Disappearing Network"
- Biologically-Inspired Services
- Self-Managed, Evolving Services to Satisfy User-Needs
- Autonomic Adaptation to Environment

Focus
- Securing Communication is not Enough
- **Match Security Infrastructures to Evolving Networks and Services!**

Many Interesting Problems to be Tackled
Summary

Setting
- Large Number of Heterogenous Devices
- Service and User Centric "Disappearing Network"
- Biologically-Inspired Services
- Self-Managed, Evolving Services to Satisfy User-Needs
- Autonomic Adaptation to Environment

Focus
- Securing Communication is not Enough
- **Match Security Infrastructures to Evolving Networks and Services!**

Many Interesting Problems to be Tackled
‘... 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.eu/

Motivations are Welcome!