Using OSGi for Secure Service Discovery

Slides available at http://godot.be/slides
Presentation Structure

- TEAHA
- TEAHA Approach for seamless interworking
- Using OSGi and Service Discovery
  - OSGi and TEAHA Features and Needs
  - OSGi vs. TEAHA Registration
  - TEAHA Security Modules
  - Architecture for Service Discovery and Security
The TEAHA Consortium

- Leading manufacturers and service companies
- Technology and market research companies and Universities
- Industry groups
TEAHA Mission

• Specify an open, secure framework for seamless interoperability and interworking

Networked Home Control Applications

- White goods
- Energy Management
- Security and Safety
- Home Controls
- Lighting Control
- Health Care for Elderly and Disabled
- Infotainment

Networked Audio-Video Applications

AV & Mobile MMI
TEAHA Has Technology Clusters

- Reference Gateway
- UPnP/WiFi
- EHS/Power Line
- TEAHA/Zigbee
- TV
- Display
- Clock
- Meter
- Security Controller
- Washing Machine
- Energy Controller
- Intrusion Detector
- Camera
- Smoke Sensor
- Oven
TEAHA Has Business Clusters

Reference Gateway

- UPnP/WiFi
- EHS/Power Line
- TEAHA/Zigbee

Multimedia
- TV
  - Clock
  - Display

Energy
- Meter
  - Energy Controller

Home Safety
- Intrusion Detector
- Security Controller

Household Appliance
- Washing Machine
- Oven

OSGi Alliance

The European Solutions Home Alliance
Facts about Stakeholders

• Stakeholders in a business cluster
  – Are competitors
  – Share the same culture
  – Are involved in the same value chain
  – Would prefer to abstract away from technology clusters

• Stakeholders in different business clusters
  – Do not understand each other
  – Do not need to understand other clusters
  – Have different cultures, value chain, life cycle
Approach for Seamless Interworking

• There are issues in supporting the mixing of different types of clusters
  – Technology clusters
  – Business clusters
  – …

• TEAHA focuses on solving those issues
Seamless Interworking Unsolved Problems

• **Service Discovery**
  - Can a device in one technology cluster discover a device from another technology cluster?
  - Can these devices use one another’s services?

• **Secure Communication**
  - Can a device in one technology cluster communicate securely with a device from another technology cluster?
    - Authenticity: No faked devices!
    - Confidentiality: No eavesdroppers!
    - Trusted/Registered devices: No intruders!

• **Security Policy**
  - Can a business cluster be protected from other clusters?
    - Policy enforcement: is a multimedia application allowed to access security system information?
Abstract Architecture

Interworking Environment

Application Framework
- Bridge Utility
- Secure Service Discovery Utility
- Secure Communication Utility

Service Framework
- Service Applications
- Service Access Utility

LAN Abstraction
- Communication Layer
- LAN 1 Proxy
- LAN 1 Driver
- LAN 2 Proxy
- LAN 2 Driver

Business Cluster Support

Security Support
TEAHA Business Cluster Support

- **Business Cluster Support**
  - **Cluster**
    - Household Appliances
      - App
      - LAN
  - **Cluster**
    - Home Safety
      - App
      - LAN

- **Plug-in Selector**
Mapping on top OSGi

OSGi Application bundles
- Service Applications
- Bridge Utility
- Service Access Utility
- Secure Service Discovery
- Secure Communication
- Communication
- LAN 1 proxy
- LAN 1 driver
- LAN K proxy
- LAN K driver

OSGi Device bundles
- OSGi Network bundles
Seamless Interworking in Action
Service Discovery in Action

Service Discovery

LAN1 Proxy

Service Discovery Proxy

LAN1 Driver

App Service Description

LAN2 Proxy

Service Discovery Proxy

LAN2 Driver

App Service Description

App Service Description

App Service Description

LAN1 Service Description

LAN2 Service Description

Service Discovery in Action

Device 1
Search for Service

Device 2
Provides Service
OSGi and TEAHA Features and Needs

- **OSGi**
  - Targets wide application area
    - Embedded and dedicated devices
  - Provides *specifications* for a service-oriented architecture
  - Defines a computing environment for *networked services* and is
    - Standardized
    - Component oriented
  - Embodies into a *service platform* with secure execution environment
  - Not supported
    - Device authentication
    - Platform management protocol

- **TEAHA**
  - Targets
    - *Home applications* and
    - *Relationships* with A/V applications
  - Provides specifications for a global home platform, focuses
    - Openness
    - Secure communications
    - Interoperability
  - Defines a middleware platform for seamless interworking of
    - Wide variety of appliances available in the home environment
    - Heterogeneous networks
  - Embodies into a logical TEAHA device
  - No open issues 😊
OSGi vs. TEAHA Registration

- **OSGi**
  - Registration of services in the OSGi platform
  - Registration with the local OSGi registry
    - Code.Bundle signing
    - Policy-based
  - OSGi services use one another’s services in the OSGi platform

- **TEAHA**
  - Registration of TEAHA devices in the wide home environment
  - Device registration requires touch & play
    - Secure zero configuration
    - Policy-based
      - Unregistered devices cannot use registered devices’ services
  - Device-Device service usage
Key Features of a Security Module:

- One SM per Device
- SM = OSGi bundle
- SM offers services to other bundles
- SM initialized by manufacturer
- Initialized SM ready to be used
- Combination of hard- and software
  - Hardware → Non-cloneable
  - Software → Risk for cloning
- Provide true strong authentication
- Secure communications rely on SM
  - Insecure
  - Authenticity
  - Confidentiality
  - Secure = Auth. + Conf.
TEAHA Security Module Services

Can be used for
- Applications
- Secure Communications

Sealed in a tamper evident enclosure, e.g., Integrity-protected log file or database, hardware enclosure,…

Functionality
- Authenticate data
- Verify authenticated data
- Decrypt encrypted data
- Encrypt plaintext data
- Generate key pair
- Generate secret key
- Play key agreement protocol
- Generate random data
- Compare Local vs. Reference time
- Convert security mechanism

Implementation relies on

inner Kernel with security features

Secure Storage
- Device/user certificate(s), data,…
- Trusted (CA) certificates
- Session data (keys, logs)

Cryptographic Engine
- Signing primitives and keys
- Decryption primitives and keys
- Secret master keys
- Decrypt and re-encrypt (optional)
TEAHA Secure Communication Types

4 Security levels:
• Protecting Integrity and/or Confidentiality

Security parameters (keys):
• Agreed on during device discovery
Secure Key Agreement with Station-To-Station

D1 broadcasts a Ping message
Ping (Session Identifier, Data (optional))

D2 sends a Pong message
Pong (Session Identifier, Data (optional))

Data Transfer
Secure Send/Receive (Session Identifier, Secured (optional) Data)

Optional Confidentiality And/Or Integrity Protection

Device + Service Discovery

Service Usage
Secure Service Discovery and Use with Registry

**Service Query**

**Direct Service Selection**

**Actual Data Transfer**
Send/Receive (Session Identifier, Secured (optional) Data)

**Optional**

**Secure P2P Discovery and Usage**

Registry

D1

D2
Master Registry issues Proofs of Registration
Strong Authentication (relying on Security Module) of Devices
Device-Device communication requires valid Proof of Registration
Example: Only one Washing Machine

Washing Machine

Wash

Ping

Ping

Ping

SM_{WM}
Residential Gateway (RG) assumes the role of a Registry Device
RG is personalized for the home
Issuing Registration Proof requires human interaction
- Physical presence of the registered device
- Knowledge of activation code of the new device
Example: Neighbor Installs Washing Machine

Neighbor’s device is not physically present ➔ Cannot receive a Registration Proof
Example: Separate Registration Domains

Neighbor’s devices receive Neighbor’s Registration Proofs
Name space reflects where a device belongs to
Conclusions

• TEAHA provides a secure and interoperable architecture for networked home applications

• Security Module is an OSGi bundle that provides
  – Secure communications services
  – Protection against cloning of the device
  – Strong authentication of the device and services

• Initialization of security-related parameters embedded in the service discovery protocol
Attend the 2nd TEAHA Open Forum
November 28, 2005
Le Méridien - Nice, France

Secure Key Agreement with Diffie-Hellman

1. Ping message sent from D1 to D2
   - Computes secret $x$
   - Calculates $\alpha^x$
   - Authenticates $\{\text{data}_1||\alpha^x\}$

   D1 Broadcasts the Ping message
   - Broadcast of Authenticated ($\text{data}_1||\alpha^x$)

2. D2 Receives a Ping message
   - Checks Authenticated ($\text{data}_1||\alpha^x$)
   - Processes $\text{data}_1$

3. D2 Prepares a Pong message for D1
   - Computes secret $y$
   - Calculates $\alpha^y$
   - Calculates $K = (\alpha^y)^x$
   - Encrypts data: $E_K(\text{data}_2)$
   - Authenticates $\{E_K(\text{data}_2)||\alpha^y\}$

   D2 Broadcasts Pong message for D1
   - Broadcast of Authenticated ($E_K(\text{data}_2)||\alpha^y$)

4. D1 Receives a Pong message
   - Checks Authenticated ($E_K(\text{data}_2)||\alpha^y$)
   - Calculates $K = (\alpha^y)^x$
   - Decrypts $E_K(\text{data}_2)$
   - Processes $\text{data}_2$

5. D1 Prepares Secure Data Transfer
   - Encrypts $E_K(\text{data}_3)$
   - Authenticates $E_K(\text{data}_3)$

   D1 Broadcasts Secured Data Transfer message for D2
   - Broadcast of Authenticated ($E_K(\text{data}_3)$)

6. D2 Receives a Secured Data Transfer message
   - Checks Authenticated ($E_K(\text{data}_3)$)

   D2 Decrypts the information within a session with D1
   - Decrypts $E_K(\text{data}_3)$
TEAHA Service Discovery

Service Discovery Kernel

- Registry mgt
- Policy mgt
- Secure Communication
- Secure Service Discovery

Service Access Utility

Communication

Security Support