e-PASTA

e-Protection of Appliances through Secure and Trusted Access

Antonio Kung - Trialog
Mario Cipriani - Merloni Elettrodomestici
e-PASTA

◆ Consortium
  – Trialog
  – T-Systems
  – Trusted Logic
  – Merloni Elettrodomestici
  – Wrap

◆ www.e-pasta.org
Context of Home Connectivity

Situation on Security

Trust Value Chains
  - Example of Service on Demand Application (Pay-per-use)

Trust through Evaluation and Certification
  - Common Criteria

e-PASTA work

Next steps

Presentation also applies to vehicle connectivity
Smart Homes will be Connected

◆ Home control
  - Lighting/shutters
  - Heating Ventilating Air Conditioning (HVAC)
  - Applications for Domestic Appliances
  - Safety and Security
  - Energy and Resource Management

◆ Communication
  - Messaging
  - Chats and Bulletin Broadcast
  - PDA

◆ Infotainment
  - Information
  - Entertainment
Several Types of Access

◆ Local
  – owner access is direct
  – owner access is through home network

◆ Remote
  – owner access is through other network (e.g. ISDN)
  – owner uses “virtual interface” (PDA, PC, etc.)

◆ Delegated
  – third party access through other network
Typical Connectivity Infrastructure

- Remote Access
- Point of Presence
- Access Network
- Gateway
- Home Network
- Appliances
- Local / Home Access
Typical Home Access

- **Dial-Up**
  - PSTN
  - ISDN
  - GSM

- **Permanent**
  - xDSL
  - Cable

Diagram:

- Node A:
  - Wireless, Broadcast
  - Satellite, RF, TV, GSM, UMTS
  - PSTN, ISDN, Power Line, Cable TV
- Node B:
  - Cable
Situation on Security of Access

- Connectivity systems are complex
- No real approach for security of access
  - not enough experience on this
  - lack of awareness
  - not all or few networks provide cryptographic mechanisms

- We need a trusted value chain
- Which guarantees that the right level of security is deployed
Trust Value Chains

Example of Merloni Pay-Per-Use Application
From the washing machine to the washing

From

- I buy the washing machine

= Washing machine

To

- I buy the washing

= Electric energy + Washing cycle + Maintenance
From the product to the use of the product

Value of the product

Value of using the product

The traditional logic of purchasing a new washing machine is replaced by a modern and smart appliance rental that enables the consumer to pay for each use, i.e. per each washing load.
The \textit{Pay\&Use} offer

- Front door delivery
- Recovery of the old appliance
- Installation and full testing
- 5 years full warranty all included
- Tele-diagnosis and Tele-allarm
- 48 hours technical assistance
- Phone assistance 7 on 7 days
- News letter with washing cycles and better use advices
First of all: a new generation of smart appliances

Capable to generate and memorize data:

- Diagnostics
- Consumption
- Historic
- Statistic

And ... ready to communicate with the outside world
A multifunction display allows access to the PXU functions:

- Residual credit
- Cost of the last washing
- Access to promotion
- Date of the last recharge
- Messages

After each washing cycle the appliance display will inform the consumer about the amount of credit left. When the credit is finished, the appliance will connect automatically to the toll-free number for re-charge. The energy consumed for each load will be automatically deducted from the energy bill.
Indoor system

- Standard model: Ariston Dialogic AD 1600
- Node for power line communication assembled at the installation transform the WM in a PayXUse version
- Telelink: modem power-line / telephone-line
Outdoor system

SOLUTIONS😊

Contact Center

→ Recharge management
→ Promotion management
→ Tele-diagnosis
→ Tele-alarm
→ SMS messages
→ Statistical data recovery

PUBLIC SWITCH TELEPHONE NETWORK

Power Line

TLI

PBX

Application Server

Call desk

Communication Equipment

Communication Manager

PXU

e-PASTA
Merloni PPU Configuration

Call Center → Gateway → Washing Machine

- Payment Server
- Application
- Payment Client

Security component

OSGI World Congress - 26 September 2002
Trust Value Chain

Consumer

Brand Guarantee

Merloni

Owner

Payment Server

Payment Client

App

Security component
Future Service-on-demand Applications

Call Center

OSGI Gateway

Appliance 1

App 1

Sec. App 2

Appliance 2

Payment Server

Payment Client

Security component

S

S

S
Trust Value Chain

- Consumer
  - Brand Garantee
    - Manufact Appliance1
    - Manufact Appliance2
      - Owner
        - App 1
          - Security component
        - App 2
          - Security component
      - Certification Garantee
        - Supplier1
          - Owner
          - Payment Server
            - Security component
        - Supplier2
          - Owner
          - Payment Client
            - Security component

- Payment Server
- Payment Client
- e-PASTA
Trust through Evaluation/Certification

◆ Use Common Criteria
  – ISO standard (ISO 15408)
  – Standard for security evaluation
    • Used for an increasing number of products (e.g. smart cards, terminals, firewalls, …)
  – Evaluation Assurance Level
    • EAL1: functionally tested
    • EAL2: structurally tested
    • EAL3: methodically tested and checked
    • EAL4: methodically designed, tested and reviewed
    • EAL5: semiformally designed and tested
    • EAL6: semiformally verified design and tested
    • EAL7: formally verified design and tested
Common Criteria Implies an Analysis Methodology

- TOE environment
- Assets requiring protection
- TOE purpose

Assumptions
- Threats
- Organisational security policies

Establish security environment

CC requirements catalogues
- Security objectives

Establish security objectives

Functional requirements
- Assurance requirements
- Requirements for the environment

Establish security requirements

Establish TOE summary specification
- TOE summary specification

Establish TOE purpose specification

Security environment material (PP/ST)

Security objectives material (PP/ST)

Security requirements material (PP/ST)

Security Spec. material (ST)
Common Criteria Imply Templates

- Notion of Protection Profile
- Reuse of Security Analysis
e-PASTA Work

- Validate approach
- Work on 3 generic configuration
  - local operations
    - e.g. start the washing machine in the home
  - remote operations
    - e.g. remote diagnosis
  - service on demand
    - e.g. pay per use

- Demonstration of security components. Technology used
  - ISO15408 for security analysis
  - Simple gateways and OSGi gateway
  - EHS home networking
Example of Conclusions on Local Operation

◆ Impact on underlying home network
  - Authentication needed
  - Encryption not needed (but could serve as authentication)
  - Denial of service protection not needed
  - Non replay needed
  - Secure initialization of keys needed
Conclusions

◆ Analyse Security Needs
  – e.g. using Common Criteria
◆ Define Security Architectures
◆ Standardise Security Components when Needed
◆ Create Trust Value Chains

Conclusions apply for vehicle connectivity