2nd UK-UbiNet Workshop

Trust within the Mobile VCE Personal Distributed Environment

Swee K. Goo, James M Irvine, John Dunlop
University of Strathclyde
What is a Personal Distributed Environment?

Imagine yourself …

**Missing List**

a) Food
   • Haggis
   • Fish & Chip
b) People
   • Mum & Dad
   • My Boss???
c) TV
   • Six Feet Under
   • Frasier

Planning a holiday

BUT,
Well…

PDE can help you to solve this problem …

Just do your record setting before you leave

WHEREVER YOU ARE, YOU CAN WATCH YOUR DOWNLOADED PROGRAMME

HOW?

Well…

PDE can help you to solve this problem …

Just do your record setting before you leave

WHEREEVER YOU ARE, YOU CAN WATCH YOUR DOWNLOADED PROGRAMME

HOW?
PDE: Devices & Services: at home
PDE: Devices & Services: on the move
Benefits of having PDE

Clearly, PDE

- optimises the usage of the distributed devices which have a diverse range of capabilities.
- primarily puts the user in control of his/her communications environment.
  - allows user to have more control access and quality for these distributed devices.
  - empowers the user to negotiate his/her service facilities and tariffs at the point of delivery.
- permits a new and diverse range of services to be delivered to the user.
- is also key in creative inter-working of wireless and broadcast technologies for enhanced service provision.
Brief Summary of PDE

PDE components

- Device Management Entity (DME)
- User Devices
  - multi-mode ‘super-terminal’
  - can act as a Network Access Device (NAD) talking to external networks
  - may join and leave the PDE in a dynamic way which promotes dynamic reconfiguration issues.

PDE structure

- can never be characterised by a fixed or a pre-defined pattern.
- largely depends on the availability of service at that particular location and time.
- PANs and wireless technologies are employed most of the time.
- As PDE’s nature is ad-hoc, the involved devices are also expected to have diverse capabilities and security threats.

These issues will cause the user to have an inconsistent view of trust in the different PDE devices.

UbiNet, 5-7thMay04
Simple Approach

‘I trust my devices’
‘I don’t trust your devices’

Trusted and Untrusted Domains

BUT

- What if a user wishes to use services on other devices?
- How does a user make a device ‘theirs’?
- What about the other parties?
  - Content provider, Network provider, etc
Trust Issues Created by PDE

Trust Specification
- Trust definition
  - What and how much trust users want and intend to define?
- Trust assignment
  - Flexibility is required; Long-term and short-term relationships
- Trust Mapping and Evaluation

From the viewpoint of …

The User:
- Can I trust all my devices?
  - Some devices I own my be more vulnerable than others
- How do I specify how much trust I place in external devices?
  - This will depend on the device and the service

Corresponding Parties:
- Can all my devices speak for me (identity)?
- Can I be trusted to obey the rules with regard to content (DRM)?
- Can my devices be hacked?
Considerations for the Trust Architecture

Who require trust functions?
- Entities that wish to join the PDE
- Entities that want to establish:
  - a PDE-internal or/and
  - PDE-external relationship(s) with other entities
- Entities that want to be assured of:
  - a device’s performance
  - the performance of the PDE’s execution system

What are the domain classifications?
- Trusted/ untrusted zones

What are the components of the Trust Engine?
- For expressing requirements for trust relations and a contemplation for identification of several security constraints
  - What is the required trust?
  - What are the criteria for setting a trust policy?
Domain Classifications

They comprise of:

- **Trusted Zone**
  - **PDE Domain**
    - Consists of devices and entities either owned or trusted by the PDE user.
    - E.g. TTP, DME, PDE devices, PDE users, event logger and billing system.

- **Service Domain**
  - Only trusted access categories are permitted to access when sufficient security procedures/mechanisms are performed.
  - E.g. computing environment, users, devices, applications, agents, data and sources.

- **Untrusted Zone** - perceived by a PDE user
  - E.g. PDE networks of other users, 3rd party device, service provider, content provider, access provider and transport provider.
General View of the Trust Architecture

### PDE Domain
- **TTP**
- **DME**
- **PDE Devices**
- **PDE Users**
- **Billing System**
- **Event Logger**

#### Intrusion Detection
- Services Audit
- Key Management

#### Security Token Exchange Service
- **Policy Expression & Exchange**
- **Security Status**

#### Trust Models (Reputation)
1. Risk Assessment
2. Recovery Rate from malicious attacks
3. Key Generation
4. Identification
5. Keeping Secrets
6. Non-interference
7. Clock Synchronisation
8. Performing Algorithmic Steps

#### Predefined Trust level (user)
- Performance Capability
  - Negotiation performance
  - Routing performance
  - System’s execution performance
- Types of Access level
- Trusting period

#### Message
- Protocols
- Bindings security

#### Security Policy/Services
- Trust Features
- Membership
- Confidentiality Level

#### Rights Management
- Security Token
- Exchange Service
- TTP
- Trust Models (Reputation)

#### Other Domain
- Other user’s PDE network
- 3rd party device
- Service Provider
- Content Provider
- Access Network Provider
- Transport Network Provider

---

UbiNet, 5-7th May 2004
Finally…

PDE shows great promise from a service viewpoint, BUT

Huge security concerns!

For the user:
- Confidentiality
- Privacy
- Trust

For corresponding parties:
- DRM
- Identity
- Trust