

Trust within the Mobile VCE Personal Distributed Environment

Swee Keow Goo, James M. Irvine and John Dunlop
 Mobile Communications Group, University of Strathclyde
 Royal College Building, 204 George Square
 Glasgow G1 1XW UK
 {sweegoo,j.irvine,j.dunlop}@eee.strath.ac.uk

The Mobile VCE project has defined the concept of a Personal Distributed Environment (PDE) of a user's devices, services and data. With an increasing number of wireless devices and access technologies available, users will be able to access their PDE in a wide variety of ways. Unfortunately, this flexibility comes at a cost - higher security risks and vulnerabilities. The traditional association with a network provider may not exist, replaced by a far more nebulous association with a number of unknown entities, network nodes and service providers. These ad hoc relationships require a notion of trust, which presents great difficulties in a dynamic wireless environment. As reported here, the MVCE project is therefore researching a trust architecture to address these issues, with the focus on aspects of trust policy formation and its evolution.

The view of the next generation has evolved from the single multi-mode 'super-terminal', to one where users access services through a wide variety of different terminals optimised for their application. These terminals, services and data that the user will access, form the user's "Personal Distributed Environment" (PDE) [1]. The PDE is a dynamic entity, changing not only with the services, but also with the location and access technology. Locally within a PDE, the different terminals that a user has available, such as cell phone, laptop, media player, etc., are likely to communicate by means of one or more personal area network (PAN) technologies. Although the PDE concept generates business opportunities for both the service providers and the network operators, it has associated trust issues between these parties and the PDE users. With distributed access to data, perhaps using shared terminals such as displays in an Internet café, the risks of unauthorised access to data or spoofing of the user are greatly increased.

Over the years, several trust management systems have been introduced. Some are developed to solve the trust issues with specific focus on general authorisation [2, 3] while others concentrate on authentication [4, 5], logic [6, 7] and particular applications [8, 9]. However, comparison between these approaches is difficult due to the fact of the breadth of these system specifications and the trust languages employed. The lack of precision introduces doubts of their suitability to specify and express the security needs both effectively and intelligently to a dynamically changing environment, with devices entering and leaving the PDE.

The ability to specify trust in a commonly understood format across domains is essential, as without this, users will not be able to trust that services offered from the 3rd

parties are safe. The frequent need to physically split and merge several different PDE networks will also makes the trust problem more complex, as each different sub-network will have its own security mechanisms (based, for example, on the access network), and its own identity server process.

The figure overleaf presents an overall fundamental structure for explicit expressions of trust relations between the entities and how the various trust policies can be created in the PDE context, with the intention of sustaining trust for:

- 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 and the performance of the PDE's execution system

From the figure, three essential domains are identified:

- *PDE Domain*: a zone that consists of devices and entities either owned or trusted by the PDE user
- *Service Domain*: a zone whereby only trusted computing environment, users, devices, applications, agents, data sources are permitted to access when sufficient security procedures/ mechanisms are performed.
- *Other domain*: an untrusted zone perceived by a PDE user. It consists the PDE networks of other users, 3rd party device, service provider, content provider, access provider and transport provider.

The crucial element in the framework is the "trust engine" which falls in between the *PDE* and the *Service* domains. Different relevant types of trust requirements can be identified and classified in this region. The trust engine depicts a formalism for expressing requirements for trust relations and a contemplation for identification of several security constraints in developing a trust policy. The trust information provided in the trust engine is time dependent and, in general, it is also varying rapidly in order to give a reliable state of information/ condition.

Six key criteria, which are considered for expressing the trust needs as input to the procedures for handling requests in the policy expression and exchange are:

- The *Trust Reputation* [10, 11] anticipates that trust establishment can no longer rely solely in just the outcome of the security mechanisms. Though direct social cues may not be available, the reputation can still be based on indirect observations or evidence from audit and intrusion detection systems.
- The *Pre-assigned Trust Level*, whereby flexibility is required in both the trust allocation and mapping.

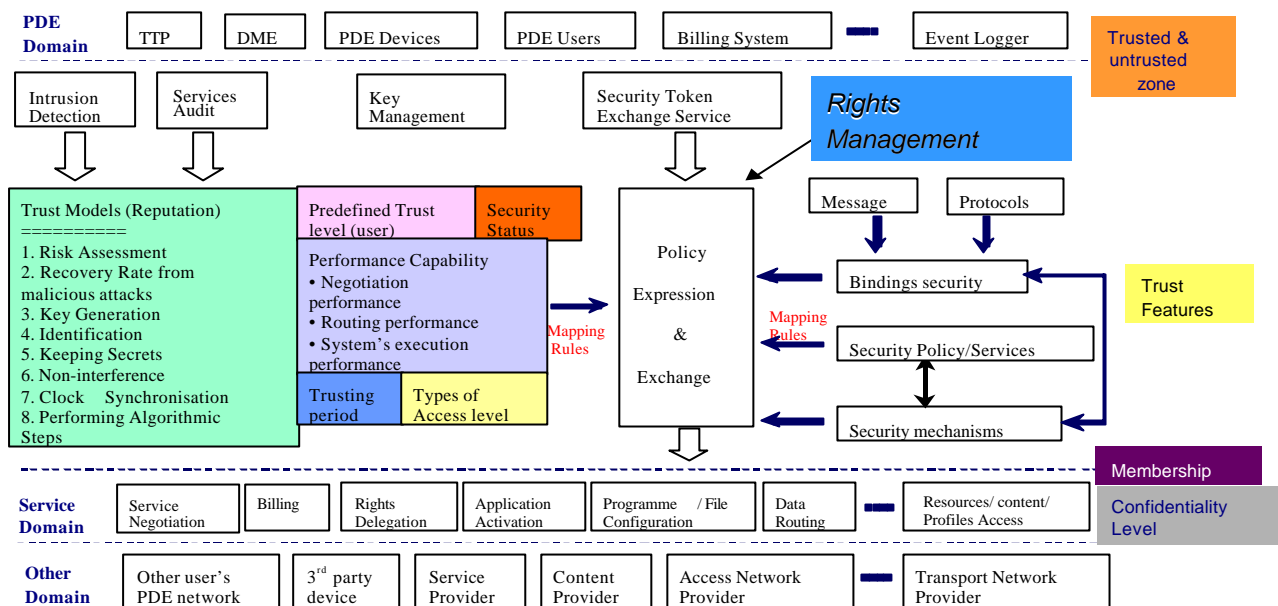


Figure: Trust Architecture for PDE

- The *Performance Capability* refers to the ability to deliver the promised services or tasks.
- The *Trusting Period* which is difficult to define quantitatively, but can have defined *Pre-Trust*, *Mid-Trust* and *Post-Trust* periods. The latter requires entity to also satisfy the security rules set by both the *Pre* and *Mid-Trust* periods before it can be permitted with the rights to access and release confidential resources and information such as user's profile, location details and monetary information.
- The current *Security Status*
- The *Types of Access* which ties with the types of required membership

The other criteria for setting up a trust policy are:

- To be effective in exchanging information on which trust decisions may be based, agreed *Protocols and Message* are also necessary.
- The *Security Policy/ Services* refers to the existed policies such as privacy policy and authorisation policy
- The *Security Mechanisms*. e.g. digital signatures
- The *Bindings Security* is to tie the security characteristics from the *Security Mechanisms* to the agreed *Protocols and Message*.
- *Policy expression & exchange* is where an ideal policy language is identified and is used to express the capabilities or any strong constraints of the PDE security. It also facilitates service requestors and providers to exchange dynamically security (among other) policy information in order to establish a negotiated security context between them.

Within the project, the trust policy work is at an early stage, but work is progressing on how policies can be generated and managed via a suitably specification language for a PDE scenario.

ACKNOWLEDGEMENT

The work reported in this paper has formed part of the PDE area of the Core 3 Research Programme of the Virtual

Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. Full detailed technical reports on this research are available to Industrial Members of Mobile VCE.

REFERENCES

- [1] Dunlop, J., Atkinson, R. C., Irvine, J., Pearce D., "A Personal Distributed Environment for Future Mobile Systems", *IST Mobile & Wireless Communications Summit*, June 2003.
- [2] Blaze, M., Feigenbaum, J., and Lacy, J., "Decentralised Trust Management", *Proc. 17th Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, 1996, pp. 164-73.
- [3] Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A., "RFC 2704 - The KeyNote Trust-Management System Version 2", 1999, <http://www.faqs.org/rfcs/rfc2704.html>
- [4] Stubblebine, S. G., "Recent-Secure Authentication: Enforcing Revocation in Distributed Systems", *Proc. IEEE Symposium on Research in Security and Privacy*, 1995
- [5] Wobber, E., Abadi, M., Burrows, M., Lampson, B., "Authentication in the Taos Operating System", *Proc. 14th ACM Symposium on Operating System Principles*, 1994.
- [6] Chen, F., Sandhu, R. S., "Constraints for Role-Based Access Control", *First ACM/NIST Role Based Access Control Workshop*, Gaithersburg, Maryland, USA, ACM Press, 1995.
- [7] Jajodia, S., Samarati P., and Subrahmanian, V.S., "A Logical Language for Expressing Authorisations", *Proc. IEEE Symposium on Security and Privacy*, 1997, pp. 31-42.
- [8] Balfanz, D., Dean, D., and Spreitzer, M., "A security infrastructure for distributed Java applications", *Proc. IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 2000, pp. 15-26.
- [9] Chu, Y.H., Feigenbaum, J., LaMacchia, B., Resnick, P., and Strauss, M., "REFEREE: Trust management for web applications", *Computer Networks and ISDN Systems*, 29(8-13), 1997, pp. 953-64.
- [10] Beth, T., Borchering, M., Klein, B., "Valuation of Trust in Open Networks", *Proc. 3rd European Symposium on Research in Computer Security*, 1994.
- [11] Goo, S.K., Irvine, J.M., Atkinson, R.C., "Personal Distributed Environment - Securing the Dynamic Service Platforms Beyond 3G", *Proc IEE 3G2003*, London, UK, June 2003, pp.18-22.