Wireless World Research Forum (WWRF)

(a) Title of the research item: Securing Personal Distributed Environments

Authors:

Name:	S. Goo, J. Irvine, R. Atkinson & J. Dunlop
Affiliation:	University of Strathclyde
Address:	204 George Street, Glasgow G1 1XW UK
E-mail:	sweegoo@eee.strath.ac.uk, j.m.irvine@strath.ac.uk

(b) Subject Area: The New Communication Environment: Security

(c) Objectives of the required research

The Personal Distributed Environment (PDE) is a new concept being developed by Mobile VCE allowing future mobile users flexible access to their information and services. Unlike traditional mobile communications, the PDE user no longer needs to establish his or her personal communication link solely through one subscribing network but rather a diversity of disparate devices and access technologies whenever and wherever he or she requires. Depending on the services' availability and coverage in the location, the PDE communication configuration could be, for instance, via a mobile radio system and a wireless ad hoc network or a digital broadcast system and a fixed telephone network. This new form of communication configuration inherently imposes newer and higher security challenges relating to identity and authorising issues especially when the number of involved entities, accessible network nodes and service providers, builds up. These also include the issue of how the subscribed service and the user's personal information can be securely and seamlessly handed over via multiple networks, all of which can be changing dynamically. Without such security, users and operators will not be prepared to trust their information to other networks.

(d) Content

Introduction & PDE Concept

In future wireless systems, it is anticipated that users will interact with a multitude of different applications using a combination of different terminals. These terminals, services and data that the user will access, form the user's "Personal Distributed Environment" (PDE) [1]. The PDE encompasses a user perspective of multiple devices (both local and remote) accessing multiple services via multiple networks, all of which can be changing dynamically. It encapsulates the concept that coverage is not necessarily universal but may occur in islands which may or may not be interconnected. This implies that a particular session may not be continuous but is commenced or continued whenever the user is within range of service delivery mechanisms which may include broadcast delivery, mobile cellular networks, low power personal ad-hoc radio networks, wireline networks, etc.

PDE is a dynamic entity, changing not only with the services, but also with the location and access technology that the user is accessing. This access technology could be UMTS, a wireless LAN, ad hoc networks and broadcast systems, or even wired gateways to a core network, but is also likely to be a combination of techniques depending on which technology is available in the current location.

A single, possibly multi-mode gateway terminal may be used, but it is more likely that the PDE will use a number of different terminals connected by one or more personal area networks (PANs). The PDE concept ensures that the users' environment is continuously customised for their needs. If a consistent set of services cannot be distributed to all the users (e.g. in a Virtual Home Environment (VHE) [2]), service modification can be attained through the PDE concept. This is a particularly versatile feature because each physical device or terminal alone will not have identical features and capabilities to meet all the instructed task requirements by the user. Hence, service modification is essential to enable suitable exploitation of the device capabilities as the volatile radio environment changes.

The PDE concept in operation may be illustrated by the scenario (depicted in Figure 1) in which Alice wishes to record her favourite TV episode while she is away from home. This is done using her home set-top box (STB) that has been programmed to record the episode from an appropriate TV network based on predefined user preferences (for instance, to view the show without advertisements at a particular price). This service, along with the STB, forms part of Alice's PDE. When the programme is recorded, the STB sends a message to Alice's UMTS handset, also part of her PDE, confirming receipt. Alice is currently travelling on a train which has a video display unit in the back of the seat, and wishes to have the programme sent to her to watch on the train. She invites the video unit on the train to join her PDE, and then instructs the STB to send the video to the train display (perhaps via the UMTS network to her handset, and then by Bluetooth to the display, or by a direct link to the train's network should the train be so equipped).

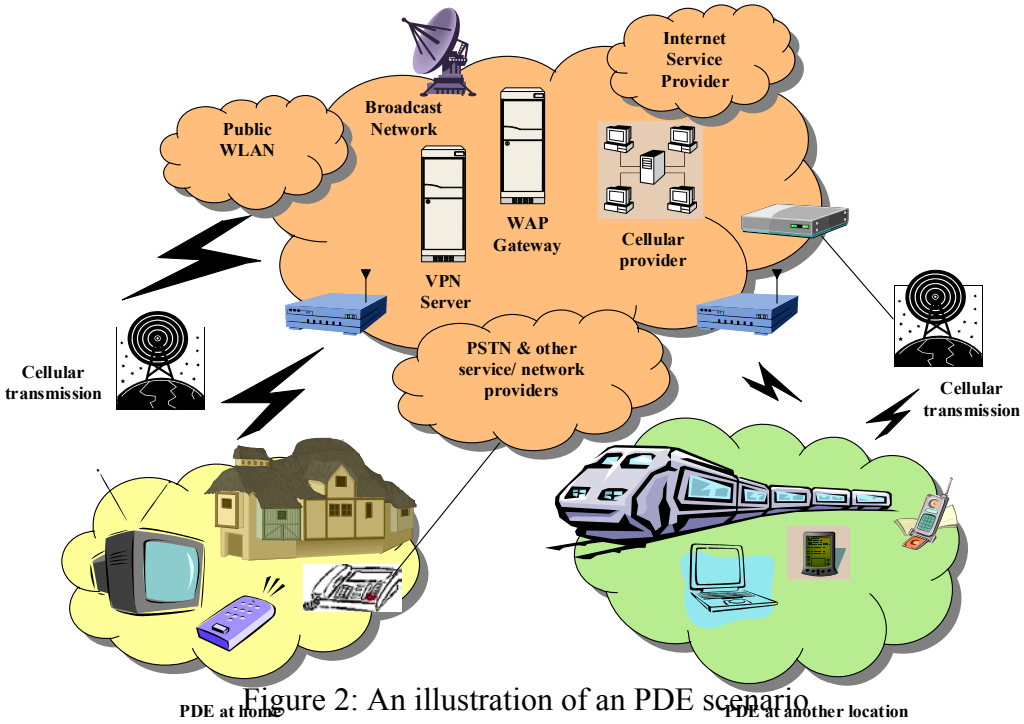

Figure 2: An illustration of an PDE scenario

While this small example shows the PDE's flexibility, as well as different opportunities for operators, it has also illustrates a number of different security concerns. The STB will still required to be authenticated by the broadcast network operator in a manner similar to current broadcast networks. If Alice has been travelling for some time, she may have instructed the STB to download any examples of her favourite programmes, rather than a specific programme at a

specific time. There are issues with authorisation and privacy similar to those in current advanced interactive TV services.

Transmission to the UMTS handset can also be done using existing security procedures within the UMTS network, but the interaction of devices is more problematic. These include how the on-train display can be securely invited to join the PDE, how private information within the PDE can be kept from the public on-train equipment, and how the transmission to the train can be authorised and paid for. Also, should someone steal Alice's UMTS handset, would having one part of her PDE allow access to information on other parts of her PDE? The content provider and broadcaster also have issues. While a broadcaster could retain control of the STB, other problems may arise when the programme is sent on to the train. How can the broadcaster ensure that its content is not rebroadcast by Alice to other users? Even if Alice does not intend to let the information leak, the broadcaster would need to trust the security of Alice's PDE. Since the PDE changes, the broadcaster is also trusting any devices that Alice trusts, such as the on-train display. If the broadcaster has sold Alice rights to a single viewing only, how can it ensure that when Alice views the programme on the train, she cannot view it again on the STB? Licensing issues may restrict the rights to certain geographical areas, preventing retransmission. How can Alice ensure that if the STB sends the programme to the train, and the transmission is unsuccessful, she can still recover it from the STB? Unless these and similar security issues are addressed, operators will be unwilling to support the PDE concept.

Current security technologies are mostly focused on specific communications technologies, and are developed by technology-specific standards bodies. These existing security technologies are not always appropriate to support the security services needed for the new complex communications configuration. This is because the operational behaviour and system configurations in these existing communication systems are very different from what is envisaged in the PDE. For example, the cellular system offers more intrasystem (and intersystem) mobility such as terminal handover between radio access nodes, than exists in today's broadcast systems, where the user simply receives and selects his or her subscribed content from a pool of resources which are broadcast. Hence, once broadcast and cellular technologies are combined to deliver user services, new security issues arise, e.g. relating to user registration to the network and handover between different network operators, that were not previously considered within the broadcast system.

Security Issues

Security for PDE can cover a wide range of possible issues affecting the link of network interconnection, and the supply of and payment for services. Security considerations and critical issues have been investigated from the perspectives of the different actors involved – the user, the network provider, the service provider and the device manufacturer.

A. User's Perspective: The primary requirement for the users is to be able to access the services they want in a secure manner, wherever they happen to be, without compromising privacy or availability. The user is unlikely to want to be involved in, or need to understand, how secure he/she wants messages (e.g. an email or a message requesting for an application), data transmissions and even the configuration of the local network security to be. With no network operator to manage the PAN within the PDE, the user is unlikely to want to take on this management responsibility, which means that PDE management must be simple and intuitive (a problem which affects more than just security services). The user's main concern remains to protect

his or her data on the fixed or mobile terminal and his or her privacy in the service interactions, specifically in service negotiation and payment transaction. A user should not be asked to pay for a service (e.g. viewing a video movie from a broadcast station) that has not been requested, but this restricts the intelligent proision of services based on prior user preferences. Basically, the discussion issues can be split into two main areas which are before and after the security volations:

i) How to avoid the security being breached in the first place?

- What is the proposed security algorithm that protects the user's information (such as identity, location, service usage profile and monetary information) from parties who do not require to know it?
- How much (and how secure) user information is stored at his subscribed service and network providers?
- When does the user need to be anonymous or use a virtual identity for which particular service transaction?
- Can the user have the option of selecting and paying for a higher security level to send and protect his or her message to an end user who is using a different service provider?
- How can the user prevent an impostor from pumping wrong information or blocking the transmission of actual data?

ii) What happens if the security is violated?

- How can the violation be recognised by user?
- How can the user rectify it?
- Can the user stop this from happening again?
- How can the user re-evaluate the trust relationship with the service provider?
- User may also need to question if the network interconnection is really reliable.
- What are the extra security measures that the user sees it requires at an affordable cost?

B. Local and Remote Networks' Perspective: If network channels are vulnerable, messages can be eavesdropped and fake messages can be injected into the network. As PDE is not always employing a fixed network configuration due to its rapid changing topology, it is important to investigate the security issues that may be encountered in this perspective. This section will involve more access security discussions such as address configuration and session key establishment that are required to support secure distribution, exchange and storage of the content. As the PDE can be both dynamic and ad-hoc at the same time, additional challenges may be imposed onto the trust model of the PDE security. This is because a central authority may not be available to assist in making trust relationships between the users and other parties in the network. Others could be:

- How can the security agent authorise other agents (e.g. mail agent) to access other networks so that the device in the PDE can receive and send data or information (e.g. email)?
- Can a tracer engage to each transaction? This is to keep track of the original recipient (i.e. network access node or router) who first received the user data when a request was established, so that it can be used for (backward) checking the unreliable route or node that releases or being hacked to release any confidential data of the user.
- In the PDE, who is in control of the authentication? The user or the service provider?

- Can the user pick his or her preferred routing path via specific devices to the recipient's final terminal? What are the security measures that the user needs?
- How can the system securely transfer or route the user information from one terminal to the other terminal for activating the (same) service retrieval?
- What types of data (i.e. high and low values) are required to be sent with security features?
- How can the data integrity be ensured?
- How much data should be stored and is it sufficient for accounting and legal purposes?

C. Service Provider's Perspective: This perspective is related to the service the user receives which may be transported over various types of networks, and may involve handovers. It concerns how to prevent and protect against data being modified from different network providers during transit. The signature protocol of the servers between different systems such as broadcast and cellular systems needs to be both compatible and securely matched while still being suitable for battery powered, low design complexity, limited memory capacity and portable devices. In this situation whereby the user's PDE changes, the service provider also needs to establish a new trust level to the user's new device (e.g. from the display of a mobile phone to a display unit on a train).

Furthermore, the security mechanisms also need to be extended from connectivity and mobility to securing the Quality of Service (QoS) of the PDE network access and service negotiation. The licensing issues (that may be regulated by Digital Rights Management) which different service providers may have enacted in their product may need to compromise the event in which the transmission (of the downloaded service) from the user's device to another PDE device may be unsuccessful and service recovery may require a retransmission of this service/ request. Among other issues there may be:

- How do we ensure and verify that the routing nodes do not misbehave or do not be cooperative?
- How can PDE prevent high vulnerability of wireless connections from attacks, such as Denial of Service?
- How can users be well protected from malicious code such as viruses?
- How can trust decisions on other parties in the network be made in the event where there is no central authority?
- How can the service provider prevent users from reselling some services (e.g. a movie clip) or forwarding them freely to their friends?
- How can masquerading be prevented when some network providers or service operators try to obtain data by deception?
- What are the security mechanisms if Denial of Actions/ Communications occurs?
- Who is responsible for the service and its security – the provider, the consumer or the transporter?

D. Manufacturer's Perspective: The manufacturer of devices within the PDE wants to ensure that its devices are as compatible as possible with other devices while being easy to use and configure. Secure hardware, such as Subscriber Identity Module (SIM) or smart card, is often used to provide

security in existing systems but network operators and service providers are unlikely to share these and designing devices to accept multiple smart cards, for example, will make them more expensive and complex. Manufacturers will also need to consider ways of configuring devices so that they can work with one or more PDEs, and not allow information leakage between them.

Security Services & Requirements

The PDE architecture is still being developed, and one of the inputs to this definition will be security requirements. Many of these are shared by ad-hoc systems in general.

A. Identification and Authentication: Since the PDE is distributed, it presents serious challenges to authentication, both of the user and of devices. Traditionally in mobile networks, user authentication is an offline activity with the user being matched to a specific device. This device is then authenticated by a SIM in a mobile phone. However, not only would such a system be very expensive to provide for every device within a PDE, there is a problem that an identity provider would be required to generate the SIM cards. Furthermore, it does not solve the problem of a user granting access of a device, which may be remote, to their PDE. As such, some forms of new identification for this piece of equipment belonging to which particular user is required when new devices are introduced/ invited into a PDE,. Only when the identity is corroborated can service and feature discovery be permitted and accessed by the user and the device.

Revocation of rights is also important. Devices invited to join the PDE should not be able to continue to gain access to information or represent the user after they have been removed from the PDE. There is also the issue of stolen terminals. Since PDEs are distributed, the concept of a Device Management Entity (DME) has been defined [1], which will know the location of different parts of the PDE. Should the PDE be physically split, each different part will have its own identity server process. While this is a flexible solution to cope with a dynamic environment as the user changes location, it raises the question of authorisation of different parts of the PDE.

In general, authentication can be used as the basis for establishing secure communications between entities. If these entities have no previous formal relationship, authentication can advantageously be implemented by using public key cryptography, where a public and a private key are used. The advantages of having public key cryptography are its 1) scalability, 2) easy key management and 3) the elimination of the need for online Trusted Third Party support for authentication. However, the users may encounter problems as to whether they have received a valid (and trustworthy) public key. By using certificates issued by a Certification Authority (CA), the problem can be solved. With the provision of CAs, end-to-end security is achieved by a Public Key Infrastructure (PKI), which involves Registration Authority (RA) and certificate repository. One example of using the same concept is a personal CA [4], which provides certificates within a PAN but without the involvement of 3rd party interceptor.

A promising approach for the PDE authentication problem is ID-based cryptography [5]. This could be used in intra-PAN communications and allows the public key to be reliably distributed without any need for public key certificates. In any case, the authentication method must be simple for the PDE user.

B. Authorisation: Authorisation is a means for users to prove that they have the rights to use something in the way they want to. This is to facilitate users, network operators and service providers with some protection from unauthorised users and any other illegitimate access. A typical security mechanism used for authorisation is server assisted signature generation protocols

[6].

The authorisation issue can also depend very much on the trust level of a device. A digital or identity based signature mechanism together with properly defined security policies for different devices, can be utilised for "legitimate" transferring or accessing of information, or running approved execution code on these devices.

C. Confidentiality or Privacy: No users would want their personal or payment details transported insecurely or made known to irrelevant parties. In order to do so, users have to safeguard their identity and location so that this information is kept in private. Authentication and other security services require the same privacy service to prevent illegal users from claiming as an authorised user to gain access. Likewise, the security mechanisms for confidentiality can be solved when authentication and key sharing mechanisms are in position. Privacy Enhancing Technologies (PET) [7] are claimed to reduce privacy related problems like trust and authentication issues.

D. Integrity: This service requirement is to avoid manipulation of data in any situations. For a network operator, when a user is granted access, a reliable relation to the user is what the operator requires. Existing techniques present in mobile networks based on symmetric cryptography can be used to address this problem.

E. Accountability: Accountability is a difficult problem to address. Different cases can be considered relating to the accountability of the user, the service provider and the network operator. In the first two cases, a reasonably long-standing arrangement may be in place which can be dealt with offline, so the problem resolves to one of identity. Should the user and service provider be unknown to each other, some form of identity provider or CA will be necessary. The problem for network operators is more complex, since as the user is moving, guaranteed service is difficult to define. This accountability problem, which is related to trust validation and reputation management can be solved potentially through Digital Marketplace [3,8].

This section is a very brief look into the fundamental security requirements. There are at least two other unexplored areas of PDE security – service availability and access control. Although the current approach to PDE security design aims to adopt a shared layer architecture with open interfaces, evaluating and re-employing the design ideas of current security technologies at specific layers, like network layer (e.g. Internet Protocol Security and firewalls) and transport layer (Transport Layer Security), will contribute to the design. Last but not least, common security standards and regulations are always needed to double ensure the deployment of PDE security.

Influence of Security Requirements to PDE Architecture: One challenge of getting the PDE security correctly is to examine how the overall PDE infrastructure can be influenced by the security issues and requirements. Examples are:

- Routing pattern of the data or how the agents transfer data from point A to point B. This also includes issues like traffic pattern and mobility.
- Conflict of having a fast mobility management protocol and a high crypto security context [9].
- Quality of Service (QoS) consideration.
- The configuration of the signalling messages at network and link layers.
- The size of the PDE network that depends on the number of implemented nodes.
- The way the PDE topology changes over time.

These short discussions place a number of restrictions on the design of suitable security mechanisms and policies for the PDE.

Conclusions

The high level PDE security requirements have much in common with security requirements for most communications systems. However, the major difference is that the PDE must also cope with interworking with a large number of different systems, each of which is likely to have its own security solution, and also a dynamic environment with devices entering and leaving the PDE. As the user requirements increase, new challenges are posed onto the security technology that provides these solutions. The PDE concept puts the user at the centre of the information environment, with all the potentials and dangers; this brings clearly many possible combinations of security mechanisms, depending on the network topologies and application configurations that must be protected.

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.

List of References

[1] Dunlop, J., Atkinson, R. C., Irvine, J., Pearce D., "A Personal Distributed Environment for Future Mobile Systems", IST Mobile & Wireless Communications Summit 2003, to be appeared in June 2003.

[2] 3rd Generation Partnership Project, "The Virtual Home Environment (Release 5)", 3GPP Technical Specification, TR 22.121 v5.3.1, June 2002.

[3] Irvine, J., "Adam Smith Goes Mobile: Managing Serviced Beyond 3G with the Digital Marketplace", Invited Paper to European Wireless 2002, Florence, Italy, February 2002.

[4] Gehrmann, C., Nyberg, K., Mitchell, C. J., "The Personal CA – PKI for a Personal Area Network", in Proceedings of IST Mobile & Wireless Communications Summit 2002, Thessaloniki, Greece, June 2002, pp. 31-35.

[5] T. Garefalakis, C.J. Mitchell, "Securing Personal Area Networks", in Proceedings of PIMRC 2002, 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Lisboa, Portugal, September 2002, IEEE, 2002, pp.1257-1259.

[6] K. Nyberg, "PAN security issues and solutions", SHAMAN Workshop – Security for Mobile Systems beyond 3G, July 2002: see http:// http://www.ist-shaman.org/

[7] Privacy Incorporated Software Agent project (PISA): see http://www.pet-pisa.nl.

[8] J. Irvine, C. McKeown and J. Dunlop., "Managing Hybrid Mobile Radio Networks with the Digital Marketplace", IEEE Vehicular Technology Conference, 2001, vol 4, pp. 2542-2546.

[9] G. M. Køien, "Network layer mobility and security management in heterogeneous (IP based) network environments", PAMPAS Workshop, Sep 2002.