유비쿼터스 사회의 보안 요구 기술+

윤찬엽*, 김광조* ,인소란**

*한국정보통신대학교 국제정보보호기술연구소, **(주)니츠

Security Challenges for the Ubiquitous Society

Chan Yeob Yeun* and Kwangjo Kim*, Soran Ine**

*International Research center for Information Security, ICU, **NITZ Corp

Abstract

Future ubiquitous communications systems are expected to enable interaction between an increasingly diverse range of devices, both mobile and fixed. This will allow users to construct their own ubiquitous device using a combination of different communications technologies. The creation of such heterogeneous, dynamic, and distributed networks raises many technical issues. This paper discusses the particular problems involved in securing such as ubiquitous environment and establishes a series of requirements that future security architectures can be based on.

I. Introduction

Ubiquitous computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user.

Security plays a vital role in developing ubiquitous applications in an increasingly interconnected ubiquitous society, where the continuous, seamless use of wireless networking and broadband technologies can ensure secure communications with anyone, any organisations, anytime, anywhere, any networks and any devices.

With the deployment of 3G mobile communications systems it is clear that future mobile devices will require access to an increasing number of services. The potential therefore exists to deliver such services to a variety of ubiquitous computing devices using a range of communications technologies. Some of these devices may be connected to form personal area networks, or PANs. Users may also have access to separate home or office networks, and third party publicly accessible devices. Taking the personal networking concept one step further, to allow interaction between personal devices using a range of communications technologies is the idea behind the Ubiquitous computing [1].

The availability of such an environment will enable wider access to on-demand services. This has obvious benefits to the consumer, the network operator, and the service provider.

Thus, ubiquitous computing (ubicom) becomes a "hot issue" for industry and academia which is currently working

+ 과기부 신기술융합사업(R&D Program for Fusion Strategy of Advanced Technologies) 니츠에서 수행하는 유비쿼터스 시스템 보안 기술 개발 과제 수행의 일부임

towards the development of secure ubiquitous applications for e-citizens. One aspect of the development of this technology that is currently under investigation is the provision of a secure environment in which to operate [2].

This paper is the initial step in the provision of a secure operating environment for the ubicom devices. To appreciate the security issues it is a good idea to begin with an overview of the concept of the ubicom itself. This is presented in section II, followed by a discussion in section III of the characteristics of this environment which present distinct security challenges. Having identified the challenges, section IV then describes what is required to secure the environment and section IV concludes by identifying potential areas of future research and work currently underway to develop security architecture for the ubiquitous society.

II. Background

The concept of the ubicom environment is based on the idea that future communications systems will allow mobile, and fixed, devices access to a wide range of services over a diversity of mobile inter-working, or collaborating,networks. The devices available to the user will form a Mobile Ad hoc network (MANET) and may or may not be available with anyone, any organisations, anytime, anywhere, any networks and any devices (A6). According to [1], the ubicom devices "encompasses a user perspective of multiple devices (both local and remote) accessing multiple services via multiple networks, all of which can be changing dynamically". The situation is similar to the WWRF concept of a MultiSphere [2] where the user has access to many different devices inter-connected by a number of gateway devices. An overview of the ubiquitous society is illustrated in Figure 1.

In Ubiquitous Society we envisage a continuous, secure and seamless use of wireless networking and broadband technologies in mobile communication, office networking, car networking and home networking. Let's look at scenarios for ubiquitous society for the e-citizens:

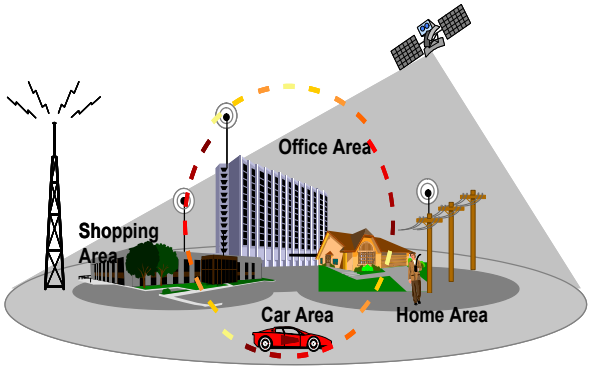

Figure 1: Ubiquitous Society Environment

- Doors open only to the authorised person.
- Rooms greet people by name.
- Telephone calls can be automatically forwarded to whenever the recipient may be or even smart enough to ask a caller to leave the Multimedia Message Services (MMS) as the recipient are busy with clients at that time
- Receptionists actually know where people are, ubiquitous terminals retrieve the preferences of whoever is sitting near at them, your virtual intelligent agents could interact with other people virtual agents to sort out the subject of a meeting as well as date and time of meetings while the people are there,
- Home intercom calls can be automatically forward to the recipients' ubiquitous terminal and he see his friends at your door at home so he can open a door and tell them to make themselves home while he/she was away for shopping at supermarket.
- By using GPS to find your friend new home and also find your friends

in the big shopping mall as well as your car has been automatically updated new traffic information and directed accordingly.

Security for ubiquitous society is illustrated in Figure 2.

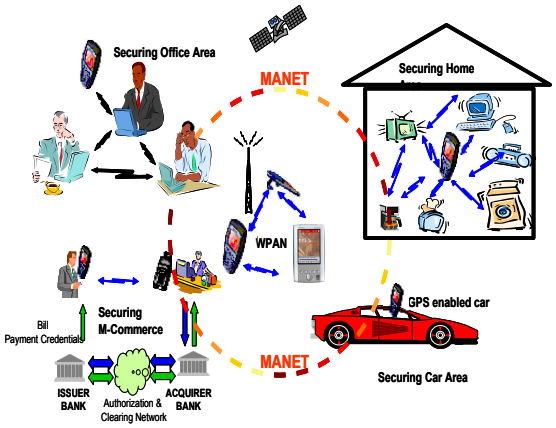

Figure 2: Security for Ubiquitous Society

One premise that the ubicom environment is founded on, is that coverage is not necessarily universal but may occur in islands which may or may not be inter-connected by collaborating networks. This implies that a particular session may not be continuous but is established or continued whenever the user is within range of service delivery mechanisms. These delivery mechanisms may include for example; broadcast delivery, mobile cellular networks, or low power personal MANETs.

The devices forming MANETs are diverse and originate in the different computing environments of the user, namely the office environment (*e.g.* company Intranet), the home environment (*e.g.* home PC, printer, STB), the car environment (*e.g.* radio, phone, navigation system), and the personal environment (*e.g.* Wireless Personal Area Network (WPAN) consisting of mobile phone, PDA, laptop, Bluetooth headphone).

In this environment a user may programme a television receiver or set-top box (STB) in the home network to monitor schedules for a particular genre of movie. Later, the user may be travelling, on a train for example, and receive a message initiated by the STB to advise him that a particular movie is just about to be broadcast. The user could receive this message either by UMTS or IEEE 802.11/802.15 and, upon receipt, reply to instruct the STB to forward the movie him. The STB would then forward the content to the user who may initially receive the service from an 802.11/802.15 connection. At some point later in the journey, the 802.11/802.15 link may no longer be available. At that point, delivery of the service may be handed over to a second network, perhaps using UMTS. The user would continue to receive the service, seamlessly, via his WPAN. Furthermore, the train operator may be able to offer the user a higher quality display than he has available on any of his mobile devices. This third party device may join the ubicom environment temporarily to provide a better display for the movie.

III. Characteristics of Ubiquitous Society Environment

Ubiquitous society environment provides mobile users with on-demand access to a wide range of services on many different ubicom devices. However, the full exploitation of such an environment will require the provision of a degree of security between participating entities. There are, therefore, a number of challenges that must be addressed to secure the environment. These challenges arise from the nature of the ubiquitous environment as described in the following.

A. Heterogeneous nature of the ubicom environment

A major objective of the ubicom environment is to integrate fixed/wired networks and mobile/wireless networks into one seamless platform. Although homogeneity may be assumed at the network layer, a wide range of technologies must be supported at the link layer, particularly where mobile devices are concerned.

The ubicom environment will also have to

support the reception of unicast, multicast, and broadcast services.

This heterogeneous nature of the environment means that a number of legacy security mechanisms will exist within an ubicom device. Moreover, the user may have a different identity and a different set of security credentials for each mechanism. The challenge is to integrate these mechanisms and manage the credentials in such a way that end-to-end security is provided to the user as unobtrusively as possible.

B. Dynamic nature of the ubicom environment

One of the incentives behind the ubicom environment is to allow mobile users to receive a wide range of services from a wide range of service providers. Many services will therefore be provided on demand and secure connections established on an ad-hoc basis.

These services will be received by a range of different mobile devices. The quality of service available to a particular mobile device will be affected by its location and the processing resources available to it. Thus to maintain a level of service, the receiver and the delivery mechanism may change, for example from UMTS to WLAN/WPAN, as the user moves around. This implies that security must be reconfigured dynamically, again with minimal user intervention.

Furthermore, mobile devices subject to limited power supplies may, from time to time, be switched off. The topology of the ubicom environment itself is therefore dynamic and devices will require authentication and authorisation as they leave and subsequently re-join the ubicom environment.

In this respect, the ubicom environment may be considered to be a logical entity implemented on a dynamic platform of devices, services, and network infrastructure. Securing the ubicom environment may then be compared to the establishment of a user-centric dynamic Virtual Private Network (VPN).

C. Trust

The concept of the ubicom environment allows the user to utilise both their own personal devices and to lease devices temporarily from third parties. Henceforth, the first category of devices will be called "home devices" and the second category will be called "foreign devices". Consequently, different levels of trust may be required for different devices, this will be reflected in the ubicom environment resources that each device is authorised to access.

D. Summary of ubicom environment characteristics

The characteristics of the ubicom environment that give rise to new security challenges may be summarised as follows:

- The heterogeneous nature of the environment means that a diversity of security mechanisms and credentials have to be integrated and managed.
- The dynamic nature of the platform raises challenges of maintaining continuity of security as the topology changes.
- Finally, there is the difficulty of establishing trust in new devices as they join the ubicom environment.

IV. Security Requirements in the ubicom environment

Having introduced the concept of the ubicom environment and described those characteristics that have an impact on security for ubiquitous society, we are now in a position to specify the requirements that

the ubicom security architecture must fulfil. The security requirements fall into three categories: general, adapted from Grid computing, and ubicom-specific.

A. General security objectives

Authentication – allows one entity to verify the identity of another entity. Often, mutual authentication is required. In the ubicom environment, we need general authentication mechanisms for user-to-device (u2d), device-to-device (d2d), device-to-network (d2n), and user-to-service-provider authentication. Moreover, we need ubicom-specific user-to-ubicom and device-to-ubicom authentication mechanisms.

Authorisation – mechanisms determine what a user can do on a device (namely the user's access rights on that device) and what the device can do within the ubicom environment. Here, we have to distinguish between home and foreign devices. For home devices, ubicom environment authorisation corresponds to the user's access rights on that device or must be a subset thereof. For foreign devices, the owner of the device delegates certain access rights to foreign users who will, in most cases, have to pay for the use of the foreign device.

Integrity and confidentiality – mechanisms have to be in place to secure ubicom-specific traffic. Moreover, ubicom management information needs to be protected in storage and during transmission.

Non-repudiation – concerns the sender and receiver of a message and is therefore required at the application level, not at the ubicom level. Depending on the specific service, it may or may not provide non-repudiation.

B. Security requirements adapted from the Grid security architecture

There are many parallels between Computational Grids and ubicom environments. The following security requirements, which originate in [4, 5], apply to ubicom environments as well as to Computational Grids.

Interoperability with local security solutions – the ubicom environment consists of devices that operate in different security domains but interact on the ubicom environment level. Local security solutions will exist in each domain but it is unlikely that they will be compatible with security solutions in other domains and at the ubicom environment level. Since these local security solutions cannot be modified, the security for ubicom environment architecture needs to interoperate with existing security solutions. The ubicom, therefore, should not attempt to impose any security mechanisms. Any security architecture proposed for the ubicom environment must be independent from specific security mechanisms.

Protection, revocation, and renewal of credentials – credentials exist at different layers of the OSI model. At the link layer, these credentials depend on the corresponding wired (e.g. Ethernet) or wireless (e.g. Bluetooth or 802.11/802.15) technology, whereas we assume IP (and IPsec) at the network layer. At the transport layer, SSL/TLS security mechanisms may be in place. Finally, the user credentials exist at the PDE level, above the transport layer, but below the application layer (where the user services run). All these credentials need to be protected, and mechanisms put in place for their revocation and renewal. Also, we have to keep in mind that, depending on the technology, the end points of the security associations differ (for example, hop-by-hop at the link layer and host-to-host at the network layer).

Single sign-on – the ubicom environment integrates existing environments, each of which has a specific authentication

infrastructure in place (e.g. Kerberos or public key based). Since the user needs to authenticate to devices, networks, and services, possibly acting in different roles (e.g. mobile user vs. student vs. on-line bookshop customer), it is necessary to implement a single sign-on solution, allowing the user to authenticate only once in order to initiate ubicom environment operations in all environments.

Uniform credentials, certification infrastructure, and cryptographic algorithms - although different security mechanisms exist in the different subnetworks of an ubicom environment, uniform mechanisms are required at the ubicom environment level. These mechanisms unify the existing solutions of a heterogeneous and dynamic environment.

C. ubicom environment specific security requirements

Global availability of ubicom management functions - the ubicom environment is a highly dynamic environment with devices coming and going. If a device acts as a gateway to a subnetwork, its loss implies the loss of the whole subnetwork. Since the ubicom environment needs to be operational despite these fluctuations, ubicom management functions need to be globally available.

Best effort operation of ubicom environment - although parts of the ubicom environment may not be operational, it is imperative that the ubicom environment works as smoothly as possible with the remaining resources.

Delegation - the ubicom environment involves many devices and services running on these devices on behalf of the user. Because of the dynamic nature of the ubicom environment, a service may change the device or the whole subnetwork on which it is running (for example, by moving from the car into the home environment). It is far too complex for the user to authorise all these changes and therefore it is necessary that the user delegates his/her rights to a management function acting on his/her behalf.

Platform protection - one incentive behind the development of the PDE is the potential to download applications to mobile devices, for example Software Defined Radio, or SDR [6], which allows mobile devices to be reconfigured over the air. Since the goal of the ubicom devices is to provide access to a wide range of services, then unless restrictions are placed on the source of downloaded applications there is a risk that malicious applications may reconfigure a device in an unauthorised manner. It is important therefore to provide some form of secure execution environment (SEE) to protect the platform from such attacks.

Content protection - another driving force behind the development of the ubicom environment is the ability to deliver new services to mobile receivers. It is envisaged that a significant number of these services will involve the provision of multimedia content. Since the digital nature of this content permits perfect copies to be made, content providers are naturally concerned that their copyright is protected. If the ubicom environment is to fully exploit the potential access to digital content, then some form of digital rights management (DRM) system will be required.

V. Conclusion

In this paper, we have addressed security challenges for ubiquitous society by listing the special characteristics of the ubicom environment that have an impact on the security architecture and by identifying the requirements that ubicom security architecture must fulfil. The complexity of the task is due to

- the heterogeneity of devices,
- the dynamic nature of the topology,
- the heterogeneity of networking technologies on the link layer (both wired and wireless),
- the fact that the new architecture needs to built on legacy security systems that are employed in the different subnetworks.

The goal of the ubicom security work is to define a global ubicom security architecture which addresses these complexities and which meets the requirements identified in section IV.

We have found many parallels between the ubicom environment and a Grid computing environment and are currently investigating which security solutions we can adapt for the ubicom environment.

Our next goal is to define the global ubicom security architecture and address isolated security research problems within it.

VI. Acknowledgement

This paper was written while I was researching security for ubiquitous computing in the International Research centre for Information Security (IRIS) Lab at ICU as a visiting research Professor. I am currently working for Toshiba Telecommunication Research Laboratory in Bristol, England as a senior research engineer. I would like to thank Professor Kwanjo Kim for arranging my visit at ICU as well as his hospitality.

References

[1] M. Weiser, "The Computer for the Twenty-First Century", in Scientific American, September 1991, pp. 94-104.

[2] R. Atkinson, J. Irvine, and S. Goo, "Personal Distributed Environment: Securing the Dynamic Service Platforms beyond 3G", in 3G2003, London, UK, 2003W.

[3] W. Mohr, "WWRF The Wireless World Research Forum", Electronics & Communication Engineering Journal, vol. 14, no. 6, pp. 283-29, December 2002.

[4] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational Grids", in Proceedings 55th ACM Conference on Computer and Communications Security, pp. 83-92, 1998.

[5] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, R.V. Welch, S. Tuecke and I. Foster, "GWD-I (draft-ggf-ogsa-sec-arch-01) security architecture for open grid services", tech. rep., GGF OGSA Security Workgroup, June 2003.

[6] W. H. W. Tuttlebee, "Advances in software defined radio," Annals of Telecommunications, vol. 57, no.6, pp. 314-337, June 2002.