A Secure and Privacy Enhanced Protocol for Location-based Services in Ubiquitous Society

Divyan M. Konidala, Chan Yeob Yeun, and Kwangjo Kim
Cryptology and Information Security Lab,
Information and Communications University (ICU),
103-6, Munji-Dong, Yusong-Gu, Daejeon 305-714, Republic of Korea.
Email: {divyan, cyeun, kkj}@icu.ac.kr

***Abstract*— This paper focuses on one of the future applications and services area of mobile communications. Mobile devices like mobile phones and PDAs would very soon allow us to interact with other smart devices around us, thus supporting a ubiquitous society. There would be many competitive service providers selling location-based services to users. To avail such services, a user's mobile device may need to handle many service providers. It should also be able to identify and securely communicate with only genuine service providers. But these tasks could create a huge burden on the low-computing and resource-poor mobile device. Our protocol establishes a convincing trust model through which secure key distribution is accomplished. Secure Job delegation and use of cost-effective cryptographic techniques, help in reducing the communication and computational burden on the mobile device. The protocol also provides users privacy protection, replay protection, entity authentication, and message authentication, integrity and confidentiality.**

I. INTRODUCTION

Ubiquitous computing [10], [9] means availability of computing and communication resources whenever and wherever we are. A Ubiquitous Computing Environment (UCE) is saturated with smart devices, which compute and communicate "for", "on behalf" and "along with" the users in order to provide some useful services. Apart from helping us to communicate, mobile devices like mobile phones and PDAs would very soon allow us to interact with other smart devices around us, thus supporting a ubiquitous society. Security plays a vital role in developing ubiquitous applications in an increasingly interconnected ubiquitous society, where continuous and seamless use of wireless networking and broadband technologies can ensure secure communications at anytime, anywhere with anyone, any organizations, 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. One premise that UCE is founded on, is that coverage is not necessarily universal but may occur in islands which may or may not be interconnected 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 *e.g.* broadcast delivery, mobile cellular networks, or low power personal Mobile Ad-hoc Networks (MANETs). Fig. 1 depicts this scenario. This dynamic nature of ubiquitous society would certainly lead to the growth of new breed of service providers who would offer Location-Based service(s) (LBSs). These service providers help the user to have continuous, secure and seamless access to closed UCE like office network, shopping malls, vehicle navigation network and home network *etc*.

Recently 3G-GPS (Global Positioning System [13]) enabled mobile phones [15] and PDAs [14] are being introduced in to the consumer market. Such mobile devices allow users to determine their current location at the touch of a button. By sending out our current location information, service providers can provide us with services "related to" and "available at" that location. Some of these services may include, obtaining a reservation at the nearest restaurant, hotel and movie theater, on-the-fly shopping, call taxi, obtaining location specific news, weather report and driving directions, and accessing your home network (washing machine, microwave, music system, car), and office network, *etc*.

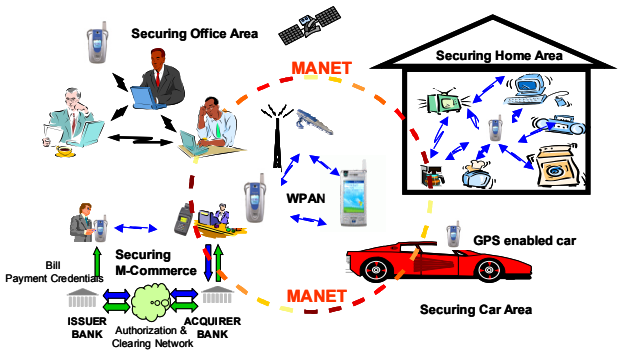

Fig. 1. Smart living for ubiquitous society

This paper has the following sections: Section II briefly describes the security requirements of our protocol. Section III, provides the overview of our protocol. Section IV, contains detailed description of the Trust Model and Setup Phase needed to execute our protocol. Section V, contains detailed description of the Location-based Service Request Processing Phase. Section VI, includes the security analysis. Section VII, compares our work with other related works. Section VIII, provides advantages of our protocol and concludes this paper.

II. Security Requirements

A. Secure Job Delegation

The mobile device on behalf of its owner may need to communicate with more than one SP. It should identify and authenticate genuine SPs and be able to secure the entire transaction and also protect the owner's privacy. But these tasks could create a huge burden on the low-computing and resource-poor mobile device and is certainly not user friendly. Therefore it would be lot easier for the mobile device to securely delegate its work to a nearby trusted high-computing and resource-rich entity, the Mobile Operator. This approach helps in reducing the communication and computational burden on the mobile device.

B. Trust Model

Establishing an efficient and a convincing trust model is very much required to ensure secure transactions, key distribution, and job delegation. With existence of a trust model, it would be lot easier for the mobile device to delegate its work to the mobile operator.

C. Users Privacy Protection

If users directly interact with SPs then they are prone to revealing their location and identity information. This information could allow SPs to generate detailed profiles of the user, his buying interests and trace all his actions. As a result restricted access to users personal data should be provided.

D. Other fundamental security requirements

Key freshness [7], Transaction Replay Protection, Entity Authentication or Identification, Message Authentication, Message Integrity, and Message Confidentiality.

III. Protocol Overview

Our protocol is simple, easy to understand, efficient and cost effective. It consists of three entities: Users (U), Trusted Mobile Operator (MO) like AT&T, BT, Vodafone, NTT-DoCoMo, *etc*, and Service Providers (SPs). A user using his GPS enabled mobile phone detects his current location. He then securely communicates his current location to MO and requests for a list of location-based services available at that location. MO replies with a list of services. It takes responsibility on behalf of users to select, identify, and authenticate the genuine SPs and also maintains a list of services they offer at a particular location. It updates this list as and when required.

User selects a particular LBS from the list and securely communicates LBS-related parameters to MO. LBS-related parameters for *e.g.* $\{CallTaxi-Service-ID, Current-Location\}$ or $\{NearestPrinter-Service-ID, File-To-Print\}$ are required to process the LBS request. MO identifies and authenticates the genuine SP for *e.g.* a Taxi Call Center and securely sends only the current location details (but not the identity) of the user to the SP. This protects the privacy of the user. SP cannot maintain the user's detailed profile, as he does not know to whom the service is being offered to. MO behaving like a "Trusted Proxy" processes the request on behalf of the user, greatly reducing the communication and computational burden on the user's mobile phone and also provides users privacy protection.

IV. Trust Model and Setup Phase

This section describes the trust model and the setup phase needed to execute our protocol. Fig. 2 illustrates this phase.

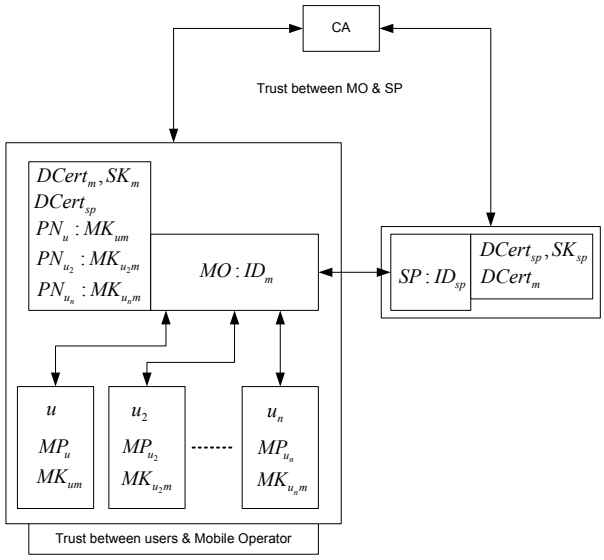

Fig. 2. Trust Model and Setup Phase

A. Trust between users and mobile operator

User installs software in his mobile phone. The software is required to execute various procedures involved in this protocol. User can either download the software through MO's official website or by approaching the nearest MO's customer service center. The software helps to generate a master secret key (MK_{um}) shared between user (u) and MO. MK_{um} is stored in the tamper resistant hardware module like SIM/USIM included in the user's mobile phone (MP_u). MK_{um} is also stored in the database of MO, probably user's mobile phone number being the index or the reference for such a database entry. As a result for all users, MO generates a unique master shared secret key. Since MO is resource-rich, storing large number of shared secret keys would not be much of a burden on it. Also, this model avoids the expensive PKI-based implementations at users end. It is very well proved in [1] that symmetric key implementations are much simpler, faster and less computationally expensive than PKI-based implementations.

1) Why Trust the Mobile Operator?: In the current mobile communications paradigm we have already put in a great deal of trust in MO, as it handles all our voice and data communications. It maintains a record of each subscriber's call details, contact information, and credit card details, *etc.* It even has the capability to easily determine our current location and tap in to our communications. But what protects us from MO turning hostile is that it has to very strictly adhere to and follow

legal, security and privacy policies imposed by the law. Our protocol extends this trust in MO to secure LBS transactions. This approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. This avoids the need to separately setup trusted proxies infrastructure to support LBSs. It is very convenient for mobile device to trust one single entity like MO rather than validating many SPs and then trusting them.

B. Trust between mobile operator and service providers

For commercial gains both MO and SPs (whom MO trusts) sign business contracts and mutually agree to provide location-based services. To secure the communications between MO and SP during the protocol execution we assume the existence of a trusted Public Key Infrastructure (PKI). MO obtains digital certificate ($DCert_m$) and private key (SK_m). Similarly SP also obtains $DCert_{sp}$ and SK_{sp} from a Certificate Authority (CA). We assume that MO and SP are high-computing and resource-rich entities. During the protocol execution they can easily, and very efficiently perform expensive PKI-based tasks like public-key encryption, decryption, and digital certificate and signature verifications. MO stores $DCert_{sp}$, which contains the public-key of SP (PK_{sp}) and SP stores $DCert_m$, which contains the public-key of MO (PK_m) in their respective databases.

V. LBS Request Processing Phase

This section provides detailed description of user's LBS request processing phase. Fig. 3 denotes this phase.

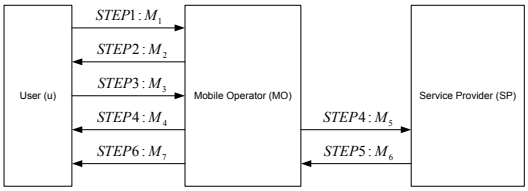

Fig. 3. LBS Request Processing Phase.

A. STEP 1

User (u) enters the secret PIN (Personal Identification Number) to authenticate himself to his mobile phone. This prevents unauthorized communications in the event his mobile phone is stolen or being tampered with. User, using his GPS enabled mobile phone detects his current location ($CLocn_u$). The mobile phone uses the master shared secret key (MK_{um}) and performs symmetric-key encryption and manipulation detection code (MDC) [7] on message M_1 and sends it to MO. $SymE_{MK_{um}}(a||H(a))$: represents the symmetric-key encryption and manipulation detection code function. M_1 represents a request from the user, for a list of available location-based services at $CLocn_u$. It contains timestamp (ts_1), phone number of the user (PN_u), unique random number (r_1) and $CLocn_u$. Using MK_{um}, user's mobile phone also generates a session key (K_{um}) by carrying out a keyed-hash function on r_1 concatenated with PN_u.

$$M_1 = \{ts_1, PN_u, SymE_{MK_{um}}(a||H(a))\}$$
$$where: a = \{ts_1, r_1, CLocn_u\}$$
$$K_{um} = H_{MK_{um}}(r_1||PN_u)$$

B. STEP 2

MO receives M_1 and also the phone number of the user (PN_u) as a part of the incoming message information from STEP 1. MO checks PN_u and retrieves the corresponding MK_{um} from its database and decrypts M_1. MO obtains r_1 and $CLocn_u$. Using r_1, PN_u, and MK_{um}, MO generates the session key K_{um}. Using K_{um}, MO performs symmetric-key encryption and MDC on message M_2 and sends it to the user. M_2 contains timestamp (ts_2), identity of MO (ID_m) and a list of services ID ($LBS_{id_1}, LBS_{id_2}, LBS_{id_3}$) available at $CLocn_u$.

$$M_2 = \{ts_2, ID_m, SymE_{K_{um}}(b||H(b))\}$$
$$where: b = \{ts_2, LBS_{id_1}, LBS_{id_2}, LBS_{id_3}\},$$
$$K_{um} = H_{MK_{um}}(r_1||PN_u)$$

C. STEP 3

User's mobile phone receives message M_2 from STEP 2. Mobile phone checks ID_m and retrieves the recently generated K_{um} and decrypts M_2. M_2 can be displayed as follows in the mobile phone:

The list of services available at $CLocn_u$ is
LBS_{id_1}: Restaurant Information Service
LBS_{id_2}: Taxi Calling Service
LBS_{id_3}: Hotel Information Service
Please Select your choice

If the user requires Taxi Calling Service, he would select LBS_{id_2}. Using K_{um}, user performs symmetric-key encryption and MDC on message M_3 and sends it to MO. M_3 contains timestamp (ts_3), PN_u, a LBS ID (LBS_{id_x}) selected by the user, LBS-related parameters ($Param - LBS_{id_x}$), which are required to process/execute the user's request by the SP and $CLocn_u$.

$$M_3 = \{ts_3, PN_u, SymE_{K_{um}}(f||H(f))\}$$
$$where: f = \{ts_3, LBS_{id_x}, Param - LBS_{id_x}, CLocn_u\}$$

D. STEP 4

MO receives M_3 from STEP 3. MO checks the user's preference LBS_{id_x}. It creates a unique random transaction ID (TR_{id}) for this particular LBS transaction. Unique TR_{id}, plays a vital role in identifying one entire LBS transaction for the user. Using K_{um}, MO performs symmetric-key encryption and MDC on message M_4 and sends it to the user. M_4 contains timestamp (ts_4), ID_m, an acknowledgement to the user stating that his request is being processed (Ack_1), LBS_{id_x} and TR_{id}. LBS_{id_x} in M_4 allows user to match TR_{id} with his earlier request.

$$M_4 = \{ts_4, ID_m, SymE_{K_{um}}(g||H(g))\}$$
$$where: g = \{ts_4, Ack_1, LBS_{id_x}, TR_{id}\}$$

User receives M_4 and obtains TR_{id}. If the user desires, he can now use TR_{id} as a reference to easily and quickly cancel this request.

Simultaneously, MO using its private-key (SK_m) and SP's public-key (PK_{sp}) sends an PKI-based encrypted signed message M_5 to SP. PKI-based encrypted signed message is represented as $PkiE_{PK_{sp}}(PkiS_{SK_m}(j))$. M_5 contains timestamp (ts_5), ID_m, LBS ID, its corresponding transaction ID (TR_{id}), LBS-related parameters and current location of the user. It can be noticed that identity of the user like his phone number is never sent to SP. It is TR_{id}, which identifies this transaction.

$$M_5 = \{ts_5, ID_m, PkiE_{PK_{sp}}(PkiS_{SK_m}(j))\}, where :$$
$$j = \{ts_5, LBS_{id_x}, TR_{id}, Param - LBS_{id_x}, CLocn_u\}$$

E. STEP 5

SP receives M_5, and decrypts it using its private-key (SK_{sp}). SP checks ID_m and retrieves the corresponding public-key of MO (PK_m) from its database and verifies the signature on M_5. Now SP knows the current location of the user ($CLocn_u$) and the LBS-related parameters. SP updates its database by including some of the LBS details like date and time, probably TR_{id} being the index or the reference for such an entry. This database entry may be used as a receipt for this particular transaction or for any payment transactions at a later stage.

SP using SK_{sp} and PK_m sends a PKI-based encrypted signed message M_6 to MO. M_6 contains timestamp (ts_6), identity of SP (ID_{sp}), TR_{id}, and LBS-related response ($Resp-LBS_{id_x}$). LBS-related response is the outcome of the user's LBS request for *e.g.* "The following taxi: XYZ 1234 has been dispatched to pick you up in approximately 10 minutes", or the map to reach your destination, or "The washing machine at your home has been switched on at 18:30 hours", *etc.*

$$M_6 = \{ts_6, ID_{sp}, PkiE_{PK_m}(PkiS_{SK_{sp}}(p))\}$$
$$where : p = \{ts_6, TR_{id}, Resp - LBS_{id_x}\}$$

F. STEP 6

MO receives M_6 from STEP 5 and decrypts it using SK_m. MO checks for ID_{sp} and retrieves the corresponding PK_{sp} from its database and verifies the signature on M_6. MO checks for the received TR_{id} in its database and retrieves the corresponding user's mobile phone number and recently generated session key K_{um}. Using K_{um}, MO performs symmetric-key encryption and MDC on message M_7 and sends it to the user. M_7 contains contains timestamp (ts_7), identity of MO, TR_{id}, and LBS-related response from SP.

$$M_7 = \{ts_7, ID_m, SymE_{K_{um}}(v||H(v))\}$$
$$where : v = \{ts_7, TR_{id}, Resp - LBS_{id_x}\}$$

User receives M_7 and stores TR_{id}, which can used as a receipt for this particular transaction or for any payment transactions at a later stage. User thus obtains his desired service via LBS-related response from SP ($Resp - LBS_{id_x}$).

VI. Security Analysis

Due to space constraint, repetitive analysis is avoided. Analysis done at each step may also apply to other steps.

A. STEP 1

1) Entity Authentication, Message Authentication, Integrity, and Confidentiality: The message M_1 provides entity authentication, message authentication and confidentiality by utilizing symmetric-key encryption. The use of one-way hash function based Manipulation Detection Code-MDC: $(a||H(a))$ provides message integrity.

2) Replay Protection: In order to get the most out of its assigned slice of the radio spectrum, a wireless system must be carefully timed and synchronized [5]. As a result in the current mobile communications scenario (like TDMA technology) the clock of the mobile phones are synchronized with the clock of MO. This aspect greatly supports the use of timestamp [7] as nonce to prevent replay attacks.

3) Key Freshness: Long-term master shared key MK_{um} is used only once at the beginning of the session to prevent key compromise due to extensive use. Instead MK_{um} is used to generate a short-term session key (K_{um}). K_{um} is used to protect the rest of the communications between the user and MO for that particular session only, thus providing key freshness. Even if K_{um} is compromised, no attacker can derive or generate MK_{um}, since the function $H_{MK_{um}}(r_1||PN_u)$ is non-reversible.

B. STEP 2

1) Replay Protection: MO verifies whether ts_1 in the message M_1 is the latest and within the acceptance window. If yes, M_1 is accepted else rejected. MO also verifies whether ts_1 inside a equals ts_1 sent in open. If both match then M_1 would be accepted else it'll be rejected. This prevents replay attack.

C. STEP 4

1) Entity Authentication, Message Authentication, Integrity, and Confidentiality: Public-key encryption and digital signatures by MO and SP provide the required Entity Authentication, Message Authentication, Integrity, and Confidentiality.

D. STEP 6

1) Privacy Protection: MO makes sure that user's identity is never reveled to the SPs. In most of the LBSs, user's identity is not required, only the location details have to be revealed. It can be noticed that TR_{id} is never sent in open. It is always well encrypted and securely communicated among the three entities. TR_{id} is used to identify one unique transaction, thus protecting user's privacy.

VII. Comparison with Related Work

Current research on ubiquitous computing [12], [16], [17] is mostly focused on closed Ubiquitous Computing Environment (UCE) like home networking or Smart Spaces. In such closed environment, interacting smart devices are mostly under the

control of a trusted server (for *e.g.* a home server). As a result every device can easily trust and securely communicate with other devices. But our protocol's trust model and secure job delegation addresses the security and privacy issues of open UCE for *e.g.*, streets, highways, ubiquitous society *etc*.

A. Identity Management

Identity Management is well described in [4]. In this approach users interact with other smart devices through pseudonyms or Virtual Identities (VID). [3] describes the drawbacks of this method. The user has to choose carefully, towards which party he uses which VID and when he has to change this VID. This approach is certainly not user friendly as it involves lot of pre-settings. It creates burden on the user's mobile device to decide and choose the appropriate VID depending on the interacting SP. In our protocol, the mobile operator conceals the identity of the user from the SP, thus reducing the burden on the mobile device.

B. Adhering to the privacy policies issued by the law

This approach is well described in [8]. [11] describes the drawbacks of this approach. W3C's Platform for Privacy Preferences Project (P3P) makes transparent use of privacy policies possible. P3P is only able to provide a technical mechanism by which services and their use of personal information are described. It does not provide mechanisms by which policies are enforced. Also it would be very burdensome for mobile device to verify such policies from different SPs and to act accordingly. In our protocol MO, on behalf of user can make sure that the SPs are adhering to the policies by verifying their claims.

C. Use of Proxies

[2] describes the role(s) of proxy in LBSs. It fails to mention about how to establish or envisage such a trusted proxy. Our protocol clearly justifies the consideration of MO to be such a trusted proxy. In [2], the proxy server acts as a SOAP Dispatcher and an intermediary between a SOAP client and the requested SP. In our protocol MO apart from concealing the identity of the user from SP, also takes responsibility on behalf of users to process their requests, select, identify, and authenticate the genuine SPs. One of the approaches in [2] assumes that the user already knows a list of trusted SPs. But in reality open UCE is very dynamic. As a result this approach is not scalable. Also maintaining and updating a list of trusted SPs and their corresponding public keys or shared keys induces a huge burden on the mobile device. In our protocol, mobile device interacts with SPs more freely with the help of MO. Mobile device neither stores a list of trusted SPs nor their corresponding keys.

VIII. Conclusion

The advantages of this protocol are as follows: Simple, involves less user interactions, secure job delegation among users and mobile operator. In case of a legal inquiry the entire transaction can traced using the unique transaction ID (TR_{id}). Mobile Operator (MO) conceals the identity of users, as a result Service Providers (SPs) cannot maintain users detailed profiles, this protects users privacy. TR_{id} speeds up the process request cancelation and current location update of walking users. Avoids expensive PKI-based implementations at users end as they have low-computing and resource-poor mobile devices. It could be a good revenue generator for the MO and SPs through commissions for every transaction. Our approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. This avoids the need to separately setup trusted-proxies infrastructure to support Location-based Services (LBSs). Since our protocol provides user's privacy protection, an extension of our protocol to include payment phase, continues to provide user's privacy protection. After availing the services or before availing the services from the service provider, the user authorizes MO to pay the SP. Later the user can settle this amount with MO via the monthly mobile phone bill. This option is very simple and can easily be implemented through our protocol. Our further work includes, extending this protocol to hide the user's LBS transaction details even from the mobile operator, thus providing complete user privacy.

References

[1] A.M. Basyouni and S.E. Tavares, "Public Key versus Private Key in Wireless Authentication Protocols", *Canadian Workshop on Information Theory*, pp. 41-44, Toronto, June 1997

[2] A.Escudero, and G.Q. Maguire, "Role(s) of a proxy in location based services". *13 th IEEE PIMRC '02*.

[3] C. Hauser, "Privacy and Security in Location-Based Systems With Spatial Models", *PAMPAS '02*.

[4] U. Jendricke, M. Kreutzer and A. Zugenmaier, "Pervasive Privacy with Identity Management", *UBICOMP '02*.

[5] P. Kuykendall and Dr. P. V. W. Loomis, T. Navigation, "In Sync with GPS: GPS Clocks for theWireless Infrastructure", `www.gfec.com.tw/english/service/content/gps_ec.htm`

[6] S. Lederer, J. Mankoff, and A. Dey, " Towards a Deconstruction of the Privacy Space", *UBICOMP '03*.

[7] A.J. Menezes, P.C. vaz Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press.

[8] G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications", *IEEE Pervasive Computing journal*, Jan-Mar '03.

[9] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges", *IEEE Personal Communications*, August, 2001.

[10] M. Weiser, "The Computer for the 21st Century", *Scientific American*, Sep, 1991.

[11] M. Wu, and A. Friday, "Integrating Privacy Enhancing Services in Ubiquitous Computing Environments", *UBICOMP '02*

[12] "GAIA - Active Spaces for Ubiquitous Computing", University of Illinois at Urbana-Champaign, `http://choices.cs.uiuc.edu/gaia/`

[13] Global positioning system overview and bibliography, `http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html`

[14] Garmins iQue 3600, the first PDA to include integrated GPS technology, `http://www.garmin.com/products/iQue3600/`

[15] Motorolas GPS enabled i205 Handset, `http://idenphones.motorola.com/iden/products/phones/phones_home.jsp`

[16] National Institute of Standards and Technology (NIST),"Pervasive Computing SmartSpace Laboratory", `http://www.nist.gov/smartspace/`

[17] "The Aware Home", Georgia Institute of Technology, `http://www.cc.gatech.edu/fce/ahri/`.