SECURITY AND PRIVACY IN A UBIQUITOUS INFORMATION SCREEN

Were Oyomno and Pekka Jäppinen
Lappeenranta University of Technology
Laboratory of Communications Engineering
P. O. Box 20
53851 Lappeenranta
Finland
{were.oyomno, pekka.jappinen}@lut.fi

ABSTRACT

In the modern city we are constantly surrounded by variety of information. Different information screens mounted at cafeterias, road sides and shopping malls display generic content which do not match often with the viewers interests and preferences. The content of the screens can take into account the preferences of the audience, by connecting to customers mobile device that runs preference providing software. When this is conducted seamlessly without specific user action, several questions towards security and privacy are risen. We present a security architecture for automatic preference transfer that protects both the service and the user from malicious outsiders. We also test the performance of our solution and show its feasibility when using handheld devices.

KEYWORDS

Ubiquitous Computing, Privacy, Security, Anonymity, Personal Information, Bluetooth.

1. INTRODUCTION

In the information society we are surrounded by information. Public screens in cafeterias, shopping malls gas stations and street corners display predetermined, cached and infrequently updated generic content that often fails to meet the informational needs of viewers. More often than not, the information is irrelevant, inaccurate, obsolete, vague and rushed. A meaningful search for information has cost and storage implications and consumes considerable amount of time and effort to filter out unsuitable data. Waiting and searching the proper information is frustrating process when vital and up-to-date information, such as sports news, stock markets, aviation reports and weather forecasts reports, are needed.

To provide accurate and meaningful information the knowledge about audience preference is imperative. Predicting individuals' preferences for determining appropriate content to screen is a mammoth task. This is primarily because individual preferences are as diverse as their backgrounds, hobbies, careers, interests and personalities. Jäppinen and Porras described preference-aware advertisement screen which relied on Mobile Electronic

Personality (ME) as preference provider [5]. Basic functionality of ME enables users' to define their preferences in advance in their mobile devices thereby facilitating their retrieval to the benefit of personalized services and customized functionalities [6]. Ferscha et al. described Digital Aura which is similar concept to exchange personal information in ad hoc manner [2].

Personalised screens are beneficial to many; especially if their operations are seamless and transparent i.e. they require no action from the user at the screen. Unfortunately, the ubiquity of their interactions, the personal nature of mobile devices, the privacy associated with users' preferences and vulnerabilities imposed by public screens, necessitates stringent security requirements if the service is to proliferate. The aforementioned solution did not take any security issues into account. The privacy protection was justified by stating that only generic non identifiable data was transferred. There were no evaluation of possible security risks nor any analysis of the implications if the security of the system is broken.

This paper presents security architecture to the ubiquitous interaction between the screen and devices running ME application. The implementation of the architecture is demonstrated to adhere to privacy and security objectives, without overwhelming the ME devices. The focus is on application level communication thus attacks involving physical threats, torture and radio jamming are not discussed. The rest of the paper is structured as follows. In chapter two we describe briefly the ubiquitous computing and ubiquitous information screen concept. Chapter three explains the security risks and vulnerabilities of the architecture. Then in chapter four we describe our solution and implementation. Chapter 5 discusses about performance of the solution and chapter six concludes the paper.

2. UBICOMP INFORMATION SCREEN

Ubicomp is a term coined by Mark Weiser [8,9] two decades ago. Its underlining conceptualization is hinged on the emergence of digital intelligence from the conventional enclosures of desktops to unconventional habitats of everyday objects, like raincoats, mugs and pets where their use remains invisible, unobtrusive and discretely calm like electricity. Ubicomp has since grown to encompass calm technology research in distributed systems, mobile computing, Wireless Sensor Networks (WSN) and Artificial Intelligence (AI). Concepts like pervasive computing, ambient intelligence and everyware emerged as closely related to ubicomp. Technological advances and innovations enabling better performance on smaller hardware footprints like embedded sensors, Radio-Frequency Identifier tags (RFID), ubiquitous networking (e.g. Wireless Local Area Networks (WLAN), Zigbee, Bluetooth, Infrared Data Association (IrDA)) have propelled ubicomp into the domains of gaming, hospitals, airports and emergency services [3].

Ubicomp information screen brings the information in our environment, always available, always visible and preferably always meaningful. The screen is controlled by service provider (SP) who gets the content for the screen from different content providers (CoP). In order to determine what is the suitable content of the screen for the current audience, the service provider has to know their preferences. Mobile device that runs ME application can act as Preference Provider (PP) from which service provider can seamlessly communicate. Viewers can define their information preferences in advance in their ME devices. Thus when they are in close proximity with the screen their devices respond to preference queries and screen show the preferred content as depicted in Figure 1.

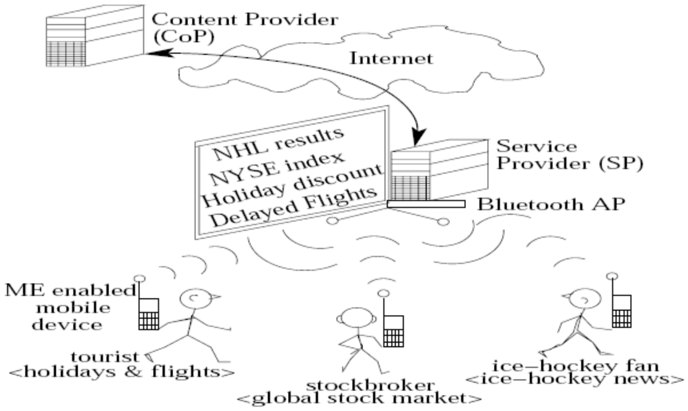


Figure 1: Information screen system

The SPs can have one or more Preference Requesters (PR) that interrogate the screen's proximity via Bluetooth's inquiry and Service Discovery Protocol (SDP) from PPs. Detected PPs are then queried over Radio Frequency Communication (RFCOMM) connection for preferred content. The request from PR contains its identity and the preference request, while the PP responds with the requested preferences. PR assimilates the responses and retrieves up-to-date versions of content from Content Providers (CoP) across the Internet. The new and relevant information for the viewers is then shown on the screen [6]. This communication is shown at Figure 2.

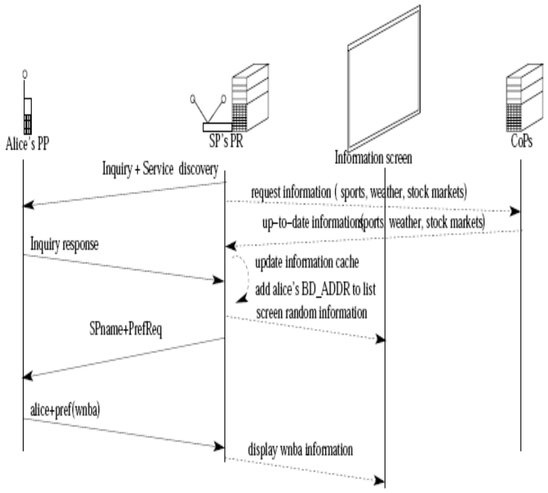

Alice's PP
SP's PR
Information screen
CoPs
Inquiry + Service discovery
request information (sports, weather, stock markets)
up–to–date information(sports weather, stock markets)
Inquiry response
update information cache
add alice's BD_ADDR to list
screen random information
SPname+PrefReq
alice+pref(wnba)
display wnba information

Figure 2: System communication

Retrieved preferences are aggregated on a scheduling policy based on the most requested information being displayed first. The personalised nature of retrieved content suggests displaying it for about 15 - 25 seconds would be sufficient time for viewers to view it. A shorter time period would compel viewers to rush their viewing of the information. The goal therefore is to limit retrieval duration within this range with the security overhead.

Viewers preferences vary in definitions, privacy requirements (favourite colour and social security number) and user perceptions (to some shopping list is private, others care little for it). Similarly, SPs can be distinguished on the basis of information they might request and retrieve (e.g. Police and marketing firm) from ME devices. As depicted in Figure 2. PP–PR interaction are in plain text, hence vulnerabilities are eminent through malicious acts such as eavesdropping, data modifications, impersonations and location tracking. If left unmitigated such malice may eventually propagate into harm, inconvenience, embarrassment or financial implication for PPs. Greenfield [3] emphasises that "ubiquitous systems must default to a mode that ensures users' physical, psychic and financial safety". These concerns should be addressed if the service is to proliferate widely.

3. VULNERABILITIES AND MITIGATIONS

PP-PR communications vulnerabilities expose the ubicomp system and its users to various compromises. Basic compromises are often layered formulating higher level attacks. To ease comprehension, the compromises are fragmented to single threats illustrated in Figure 3. Actors are also used to differentiate adversaries. At the same time, a numbering has been adopted to enforce logical analysis. Furthermore, attack modes are categorised into active attacks (solid lines) and passive attacks (dashed lines). The latter suggests indirect involvement of adversaries in the communication protocol while the former implies adversaries actively attempt to alter the protocol to their advantage.

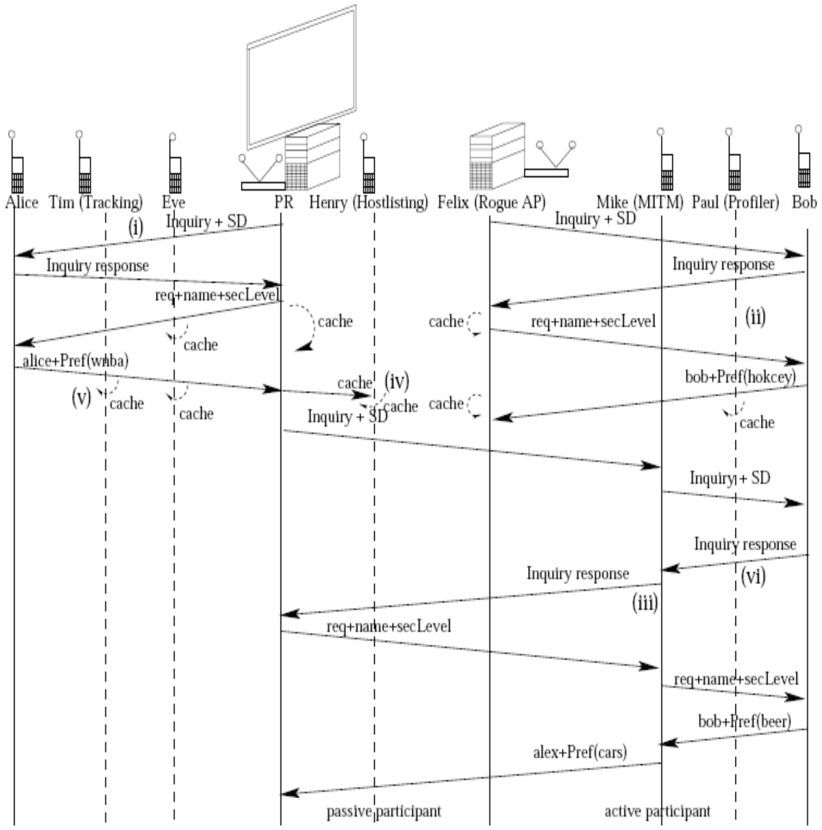


Figure 3: Information screen vulnerabilities

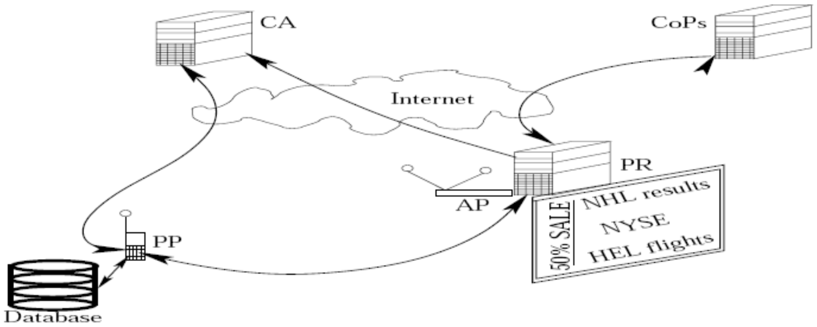
Vulnerability (i) in Figure 3; eavesdropping, is mitigated using encryption. However, performance requirements and key establishments instigate a disapproval of asymmetric encryption. Key establishment schemes leading to mutual involvement are desirable because they permit creation of securely shared secrets e.g. Diffie-Hellman (DH). Felix's PR's impersonations (vulnerability (ii)) necessitate authenticating PR via public-key certificates. This requires Trent, a Trusted Third Party (TTP) acting as a Certificate Authority (CA). In compromise (iii) Mike alters transmitted Bob's preferences from *'beer'* to *'cars'*, in deterring this malice we a need mechanism enabling the integrity of received messages to be verified. This is accomplished using hash functions via digital signature. It is also evident that Mike goes beyond message alteration to a Man-In-The middle (MITM) compromise. MITM is a complex double-faced compromise mitigated by enforcing both participants to satisfactory prove their identity. This requirement forces Bob to install secured certificate from Trent, and to frequently verify if it still validly mitigates MITM.

Deterrence of passive attacks requires additional mechanisms beyond cryptography, though along with it. Threats (iv)–(vi) involve hotlisting, tracking and profiling PPs using static transmitted identifiers. By introducing PP anonymity deters them. Adopting pseudo identities, randomly indistinguishable on different sessions and using message digest rather than signature from the PP for integrity checks mitigates the malice. Misbehaving PR administrators can also compromise the PP security and privacy, if they access information exceeding their security clearance. This malice results in disclosure of private data, such as addresses, phone numbers and identity that can be effectively used for target marketing leading to PPs privacy invasion. This is mitigated by the PR not storing any personal information beyond its use.

4. IMPLEMENTATION

Deterrence of PR-PP communication vulnerabilities necessitates adopting resource efficient algorithms like Elliptic Curves Cryptography (ECC) and Advanced Encryption Standard (AES) [7]. ECC is based on Elliptic Curve Discrete Logarithmic Problem (ECDLP) as opposed to integer factorizations [1]. This implies a fully exponential running time to offer same security level with shorter keys than sub-exponential running time of integer factorizations. Thus a 160-bit ECC key offers the same level of security as a 1024-bit Rivest, Shamir and Adleman (RSA) key. Smaller keys in the for PR–PP interaction result in faster cryptography, do not overwhelm the constraint mobile devices and, are efficient on storage and bandwidth usage [1, 4, 7].

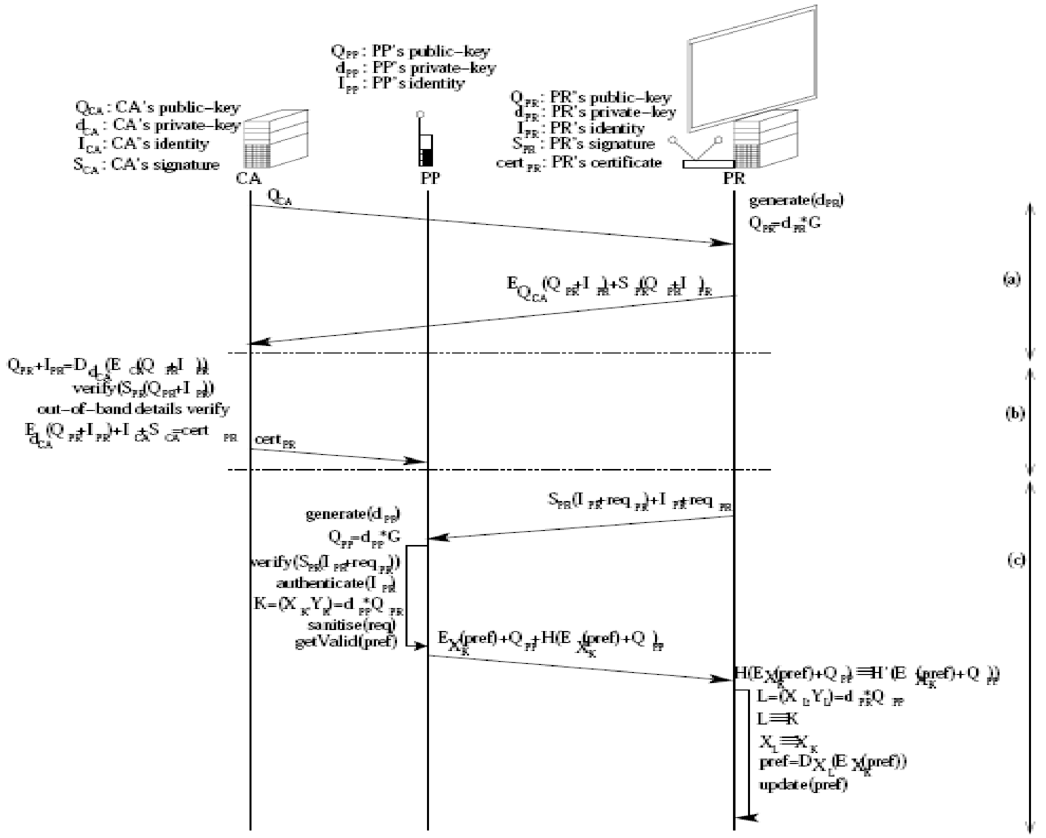
Secure PR–PP implementation makes two new additional requirements necessary: a CA and a Database. The CA implements an X.509 variant of public-key certificate based on ECC while the database is a light weight server-less variant called SQLite3. The certificate identifies the PR exhaustively while detailing domain parameters and utilised curves (e.g. NIST 192 and NIST 224). The PR credential are verified out-of-band by the CA to such an extend it is infeasible to be impersonated. SQLite3 is mainly used for access control and anonymity management. Figure 4. depicts this architectural setup.



4.1 Secure interactions

Interactions in Figure 5. begin by PR being registering in the CA through signing and encrypting his credentials when sending them to the CA part (a). CA verifies these details prior to publishing them in the form of a PR's certificate, $cert_{PR}$ part (b). For PPs to request information services from a PR they approve the service from the CA. Approval involves downloading an installing the $cert_{PR}$ as part (b) depicts. Once in possession of $cert_{PR}$, PR and PP parameters are synchronised. Viewers then configure their PPs to appropriate privacy requirements that involve settings of permitted SPs and access level control in the database. The PP on entering the screen's vicinity in discoverable mode results in the PR discovering it and requesting preferences by transmitting a signed copy of its identity and the preference request ($S_{PR}(I_{PR}+req)+I_{PR}+req$). This stage of the interaction is based on ECDH algorithm. Thus, despite any adversaries acquiring the information, they cannot formulate any compromise with it.

On receiving the transmissions the PP verifies its integrity using the Elliptic Curve Digital Signature Algorithm (ECDSA) and formulates its public-key (Q_{PP}). If the signature is valid then next step involves the formulation of shared session-key (X_K) for use with AES. The request is then sanitised and the response retrieved from the database. The PP encrypts its response with X_K and computes a digest of its public-key and the ciphertext. PP then transmits encrypted response ($E_{X_K}(pref)$), Q_{PP} and the digest ($H(E_{X_K}(pref)+Q_{PP})$) as illustrated in part (c). PR on receiving the transmission also conducts some computations to eliminate any malicious intent. Firstly, the digest is verified before Q_{pp} can be used to formulate the session-key (X_L) that is then used to decrypt the preference. Once the preference has been decrypted, the preferences are updated. Thereafter, the PP is able to view their preferred content. Attempts have been made to minimise the security overhead in the implementation by reducing and eliminating unnecessary information exchanged in the communication.



Q_{PP} : PP's public–key
d_{PP} : PP's private–key
I_{PP} : PP's identity
Q_{CA} : CA's public–key
d_{CA} : CA's private–key
I_{CA} : CA's identity
S_{CA} : CA's signature
Q_{PR} : PR's public–key
d_{PR} : PR's private–key
I_{PR} : PR's identity
S_{PR} : PR's signature
$cert_{PR}$: PR's certificate
CA
PP
PR
Q_{CA}
generate(d_{PR})
$Q_{PR}=d_{PR}*G$
$E_{Q_{CA}}(Q_{PR}+I_{PR})+S_{PR}(Q_{PR}+I_{PR})$
(a)
$Q_{PR}+I_{PR}=D_{d_{CA}}(E_{CA}(Q_{PR}+I_{PR}))$
verify($S_{PR}(Q_{PR}+I_{PR})$)
out–of–band details verify
$E_{d_{CA}}(Q_{PR}+I_{PR})+I_{CA}+S_{CA}=cert_{PR}$
$cert_{PR}$
(b)
$S_{PR}(I_{PR}+req_{PR})+I_{PR}+req_{PR}$
generate(d_{PP})
$Q_{PP}=d_{PP}*G$
verify($S_{PR}(I_{PR}+req_{PR})$)
authenticate(I_{PR})
$K=(X_K,Y_K)=d_{PP}*Q_{PR}$
sanitise(req)
getValid(pref)
(c)
$E_{X_K}(pref)+Q_{PP}+H(E_{X_K}(pref)+Q_{PP})$
$H(E_{X_K}(pref)+Q_{PP})\equiv H'(E_{X_K}(pref)+Q_{PP})$
$L=(X_L,Y_L)=d_{PR}*Q_{PP}$
$L\equiv K$
$X_L\equiv X_K$
$pref=D_{X_L}(E_{X_K}(pref))$
update(pref)

Figure 5: MSC for secure preference transfer

5. PERFORMANCE AND EVALUATION

Performance measures investigate implemented security mechanisms overhead as part of the ubicomp systems vulnerability assessment. These measures are compared on the system profiles depicted in Table 1.

Table 1. System profile of machines used in the performance and evaluations of ubicomp screen security.

System name	OS	CPU	RAM	Bluetooth radio	Role
Nokia N770	Linux 2.6.16	ARM 252MHz	64MB	v1.2	PP
Desktop PC	Ubuntu 7.10 Linux 2.6.22-15	AMD XP 1700+	757.4MB	v1.2/v2.0	PP/PR
Notebook PC	Ubuntu 8.04 Linux 2.6.24-16	PIII 1133MHz	1002.7MB	v1.2/v2.0	PP/PR

The PC machines used are not high end products. This is in line with what a realistic processing that mobile devices are likely to attain in the near future. Performance is benchmarked and tabulated against three timing aspects; PP-PR connection time, request–response time and total time. PP-PR connection time is a measure of the time it take for parties to establish a RFCOMM connection, while the request-response deals with how long the PR has to wait after requesting some preference. Total time deals with the entire time duration before the PP may view their selected content, inclusive of all overheads. Measures are in seconds. Table 2 and 3 depict insecure setup while last 2 are secure setups.

Table 2. PR (Notebookv2.0) – PP (desktopv1.2) insecure screen.

connection time (secs)	response-request time (secs)	total time (secs)
0.071	0.112	1.292
0.086	0.120	1.405
0.082	0.174	1.387

Table 3. PR (Desktopv2.0) – PP (N770) insecure screen.

connection time (secs)	response-request time (secs)	total time (secs)
0.084	1.477	2.626
0.083	1.563	2.956
0.075	1.493	2.253

Table 4. PR (Notebookv2.0) – PP (desktopv1.2) secure screen.

connection time (secs)	response-request time (secs)	total time (secs)
0.055	0.691	2.174
0.042	1.051	2.280
0.046	0.879	1.836

Table 5. PR (Desktopv2.0) – PP (N770) secure screen.

connection time (secs)	response-request time (secs)	total time (secs)
0.087	12.996	14.029
0.083	12.776	14.224
0.084	12.892	13.801

Tables 2 and 3 insecure environment averaged 1.361 and 2.612 seconds respectively for total time while, for secure counterpart similar setups averaged 2.097 and 14.018 seconds. The demonstrates that despite the increase in values due to security overhead they were still less than the 15-25 seconds window, hence makes them practical in use.

Cryptographic evaluations of the secure screen's transactions in Figure 5 followed the same 3 parts for consistency. Vulnerability assessments revealed that parts (a) and (b) are similar to mechanisms used in Hypertext Transfer Protocol over SSL/TLS (HTTPS). The mechanism has been successfully implemented in Internet banking and E-commerce applications. Thus, we anticipate the same level of stringent security here. This renders the potentially vulnerable part being the part (c). Adversaries trying to compromise the screen will most likely begin by installing cert$_{PR}$ and then eavesdropping on PP-PR interaction acquiring Q_{PP}, $E_{X_K}(pref)$ and $H(E_{X_K}(pref)+Q_{PP})$. Using the data they attempt to recompute X_K - a futile act amounting to attacking ECDH algorithm that has being proved to be computationally infeasible with current technology. The infeasibility applies also to attempts to forge the signature or modify data as the signature and the digest easily reveal inconsistencies. Thus, MITM and impersonations are sufficiently mitigated. Adoption of adjustable privacy mechanism makes PPs output anonymous such that after encryption they are indistinguishable. This means PP cannot be tracked, monitored or linked to a particular viewer. Use of access control through the database eliminates potentials for abusive PRs' as does the sanitation of request rid of potential SQL injections attacks.

6. CONCLUSION

This paper presented the ubicomp information screen environment, emphasising its ubiquitous interactions with ME devices. Despite demonstrations of the ubicomp being beneficial to many it was apparent that without consideration of its privacy and security issues, these would be reduced to a mere handful. Suitable security architecture has been modelled and implemented. The implementation has also been demonstrated to attain set security and performance objectives.

While majority of security concerns were mitigated, issues such as tracking based on underlying transport media (Bluetooth device address (BD_ADDR)), Denial of Service (DoS) attacks involving sending of garbage to the PR, and exhaustive attacks on the PPs should be considered in future works. As should security layer's performance on different mobile platforms (e.g. Symbian) should be investigated.

The demonstrated secure ubicomp screen has been presented as suitable for fulfilling our informational need especially when mounted in public vicinities like cafeterias, shopping malls and gas stations. Additionally its concept can be extended to advertisement model that result in the users viewing advertisement they prefer as opposed to SP posting advertisements they think users need.

REFERENCES

[1] Blake I. F: Advances in Elliptic Curve Cryptography, volume 1. Cambridge University Press., 2 edition, 2005.

[2] Ferscha, A., Hechinger, M., Mayrhofer R, dos Santos Rocha M., Franz M. and Oberhauser, R., Digital Aura, Proceedigns of Pervasive 2004, Springer Verlag, 2004

[3] Greenfield A: Everyware, The dawning age of ubiquitous computing, volume 1. New Riders, 1 edition, 2006.

[4] Hankerson D. et al: Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc, 2004.

[5] Jäppinen P. Mobile Electronic Personality. PhD thesis, Lappeenranta University Of Technology, 2004

[6] Jäppinen P., Porras J., Preference-aware Ubiquitous Advertisement Screen, IADIS International Conference e-Commerce 2007, pp. 99-105, December 2007, Algarve, Portugal

[7] Shar A. M: Elliptic curve cryptography, an implementation tutorial. Tata Elxsi Ltd, 1(1):1 – 11, 2000.

[8] Tripathi A. K: Reflections on challenges to the goal of invisible computing. Ubiquity, 6(17):1–1, 2005.

[9] Weiser M: The computer for the 21st century. In Scientific American Journal, pages 94 – 104, New York, NY, USA, 1991. ACM.