December 2002

Location Awareness and Privacy in Pervasive Applications

Alexander Ng
Monash University

Arkady Zaslavsky
Monash University

Location Awareness and Privacy in Pervasive Applications and Their Impact on Resource Constraints

Alexander Ng and Arkady Zaslavsky

School of Computer Science and Software Engineering
Monash University
Melbourne, Australia
ang@csse.monash.edu.au

Abstract

The ability to 'smartly' ascertain and adapt to the context of a situation or scenario is known as context awareness. A significant element of context aware systems lies in the use of location based services. Location is an important contextual parameter in context aware computing, and can affect various modes of interaction between user and application. With the increased use of data services in mobile computing today, wireless security is paramount and lacking. However, the use of location parameters is also closely tied in to security issues such as security, privacy and resource usage problems on mobile clients. In this paper, we discuss the relationship between location and security and our design of LOCAS, which is a location aware adaptive security model that scales various 'profiles', or grades of security depending on resource levels. In addition, some m-Commerce and scenarios for location-based services involving security and privacy are also discussed.

Keywords

Context Awareness, Location, Privacy, Security, Resource management

INTRODUCTION – CONTEXT AWARENESS AND LOCATION

The popularity of portable computers coupled with the immense growth of mobile voice/ data services in the telecommunications field, has made the catchphrase "information access anywhere anytime" a reality. This has enabled convenient access to fieldwork, enterprise resources, real time collaboration, and web commerce while being constantly on the move. However, as mobile computing takes off, issues such as smaller screens, different web standards (such as WML, XML, CHTML) and device capabilities, manifest in today's computing world. Lack of device adapted content, inadequate bandwidth, and a volatile wireless environment continue to plague users and application service providers. As this technology to roam between wireless networks becomes increasingly uncommon, issues such as security and privacy become glaringly mandatory to users who receive and transmit data over the airwaves. The open and dynamic nature of the Internet boom over the recent years has made information security a mandatory aspect that cannot be ignored in any information system or enterprise. With the parallel growth of pervasive computing, security for the mobile Internet never seemed further away. Even in its seedling stages, security and privacy concerns in mobile computing have been strongly voiced and contested. However, although both privacy and security are often discussed or seemed related, in truth, they are separate issues. Security is a solution, and a deterrent against threats to any entity in cyberspace. Bruce Schneir (author of crypto algorithms Blowfish and Twofish) once said, "Security is a process, not a product" and should be a means to an end solution (Privacilia.org *www.privacilla.org/fundamentals/security.html)*. It is only, when security is not enforced correctly, that will lead to a violation of an entity's privacy commitments. Privacy on the other hand implies the rights and social ethics of the computing industry, and how it affects the way in which we live for instance. Security when implemented incorrectly will typically lead to privacy infringements (such as the theft of intellectual property or information) and the compromise of an organisation's system integrity.

The nature of wireless communications and the security of mobile data carry risks to any mobile user. This is because mobile computing or mobility is characterised by wireless networks that are heterogeneous, dynamic and scarce in resources (Lubinski, 1998). As such, mobile services and applications need to *adapt* according to context of the environment. This is so that the use of resources is optimal and user experience is not

marred (for example by bad presentation, or even data corruption). Context is becoming increasingly important in handheld and ubiquitous computing, where the user's context often changes rapidly. Discovering and taking advantage of contextual information and adapting an application's behaviour to a user's context is known as *Context Awareness*. Because handheld devices are often constrained by resources, the use of adapting in context awareness will enable mobile applications to extend their limited capabilities (of both client and software). The challenge for mobile applications is to therefore effectively make use of contextual information to affect *security*. Chen and Kotz (1999) define context aware computing as a way for which mobile computing applications are able to discover and take advantage of contextual information (such as user, time, location, people and devices in proximity, user activity and preferences) through the environment. Context awareness juggles various parameters to provide the best experience possible. This is difficult because a context aware system needs to perpetually monitor the environment and resource levels.

Context Awareness encompasses a broad umbrella of items. Three important features of context awareness are "where you are", "who you are with" and "what resources are available" (Schilit *et al*., 1994). This paper discusses the location aware aspects ("where you are") and its relation to mobile data security. In addition, we will discuss the issues hampering mobile security, and how location awareness and resource constraints affect its implementation. Furthermore, we also describe the motivation and background to our work in progress and the concepts involved.

"Where am I? Am I safe now?"

Security in the computing field is considered an end-to-end solution, and should always be a concern when sending or receiving sensitive data. This is fundamental in any computing scenario, and applied no differently to the world of pervasive computing. The crucial 'last link' of any wireless network usually spans the distance between the mobile client and the base station or access point. It is at this link that security should be at its strongest (securing the crucial 'last mile' data pipe between client and base station), where physical security is at its weakest. This is especially important, given the constraints in the wireless field where slow CPU power, limited battery capacities, different screen sizes, slow bandwidth and the unpredictable physical environment make writing mobile applications are a complex process.

In any physical environment, a location change usually denotes a change in security levels. For instance, there are physical locations that are safer then others, e.g. a certain street that you would rather take on your way home instead of walking through a dark alley shortcut. Other instances relate to how safe you feel when carrying around important or sensitive data, for example, opening a suitcase of money in public as compared to doing it in the safety of a bank vault. A final third example relates to a scenario faced by fighter pilots known as 'Situational Awareness'. Similar to context awareness, situational awareness in a dogfight translates to *location* awareness (i.e. "where is the enemy plane now?" "Is it behind or is it above me now?"). With a comprehension of situational awareness, a fighter pilot's safety (i.e. security) can be preserved as long as he knows where his location is, relative to the enemy. Therefore, situational awareness can be likened to context awareness whereby a subject is acutely aware of the circumstances surrounding it. The added advantage of a subject being conscious of its location, improves its ability to react or adapt to circumstances. Such circumstances could include measures taken to safeguard the subject's security.

In the abovementioned paragraph, the situations we described, relate physical security to location awareness, furthermore we also mention that location plays a crucial determinant of safety. However, in mobility, the data security of a mobile device is affected by both its context and the physical geographic location in which it resides in. Mobile devices operate in environments more hostile and unstable as compared to a wired desktop contained by a protected office LAN. Hence, different security policies are needed for wireless networks.

Briefly mentioned below are some issues that will affect data security in a wireless network medium:

- Use of resources by persons not authorised to access network resources wirelessly across different domains.
- 'War-driving', which primarily consists of eavesdropping activities by attackers, armed with satellite or mobile dishes.
- Due to the different physical nature of wireless communications, bandwidth is less static then a wired connection. These are usually caused by fluctuating signal to noise ratios, mobile network coverage reception, presence of obstructing physical objects and mobile cell limits.
- Different base stations have different security levels and protocols. This is usually encountered in the case of a mobile user who hops between different network access points or base stations. Wireless WANs are generally less secured then WLANs due to the wider coverage and more costly infrastructure nature (although this is not a always the case). As a result, different security and privacy guarantees are offered.
- Unexpected disconnections – These are usually caused by a low signal reception or a sudden black out in cell coverage. Disconnections or partial connections result in loss of data and error recovery.
- The integrity and confidentiality of information is a mandatory concerned whether in wired networks or wireless networks.
- Privacy in location aware systems will constantly be subjected to issues of user anonymity, as users may not prefer to be tracked nor be constantly bombarded by unnecessary services.

In pervasive computing, location identifies where the mobile device is within a mobile space. A crucial determination of *context* for a mobile unit is by its location and its current physical environment. Hence, this environment affects the security of a mobile client's data, because a change in context is usually associated with a user's movement. Consequently, a change in location can therefore imply a change in context. Figure 1 shows the relationship shared between, *context awareness*, *location awareness* and *security.*

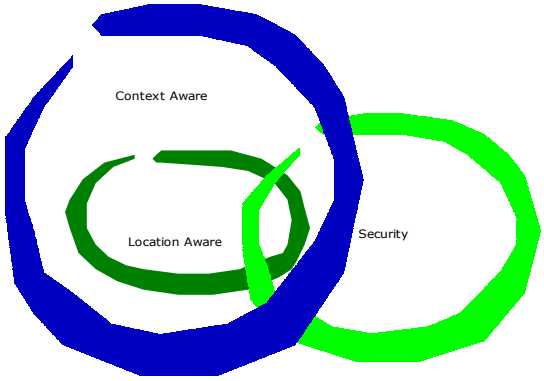

Figure 1: Relationship between context awareness, location awareness and security

Because today's handheld and mobile clients are limited in resources (such as limited memory capacity and processing power) and constrained by the fundamentals of the pervasive environment, designers of mobile applications should be mindful of limitations forced upon the device and its software. A 'one size fits all' notion should not be applied since different levels of security are needed for different services. This axiom should be applied to the pervasive computing world, since utilising security features when not necessary or needed would put additional constraints on the device and system. Selecting different encryption algorithms/ solutions would allow better use of processing power on the client side or alternatively simply 'push' the heavier processing to the server as much as possible. However, having "IF-ELSE" policies concept might be too simplistic in attaining optimal operational strategies in pervasive computing. This is because merely selecting *preset* encryption solutions for adaptation might not provide sufficient granularity in determining the correct levels of security needed to enforce a wireless connection.

Outline of Paper

Security in pervasive systems has focused on implementing models that would best suit a mobile environment. However, the challenge is to determine and identify the tradeoffs in resources between security and expressive power (Roman *et al.*, 2000). The limited amount of bandwidth, battery power and CPU processing speeds on today's mobile clients prevent the full use of resource intensive encryption to maintain data integrity and anonymity. As a result, these devices are restricted to simpler computing tasks.

After some amount of investigation, it has been noted that little has been discussed about the security and location aware relationship (aside from privacy and access control lists). In addition, we have not seen any written publication that describes a 'balancing act' required in resolving security, location and resource constrain issues. A need for adaptive security control mechanisms in location aware mobile applications is critical. This is specially beneficial and useful in a system where resource constraints are a key consideration in adapting security to location information.

In this paper, we illustrate a relationship between the use of *Location Aware* systems, how it can affect the *Security* of a device and in turn how resource management systems can be used to vary the necessity and amount of security needed by scaling through a 'threat level' system. Also discussed in this paper is our proposed approach from which Location Aware Systems can adapt different measures to security and privacy. Termed LOCAS, short for LOCation Adaptive Security, LOCAS is a location aware security model that adapts a system's security levels according to the location of the client and the resources available.

LOCATION AND SECURITY

Touted as the next killer application (Robinson, 2000) in mobile e-Commerce, Location Based Services (LBS) have started finding their way into enterprise and business applications. Japanese phone companies such as J-phone are among the very first to introduce location based services to their subscribers. Location based service cellular services include locating the nearest Post Office, bank or supermarkets (depending on the user's current location). All of which will become increasingly common as the Mobile Internet garners speed. Besides useful navigational purposes, with LBS, delivery of personalised real time location-based content becomes a reality. With m-Commerce, privacy control in pervasive systems is especially important, because of the ease in which location information can be disseminated. Hence, it is vital to design systems that allow a user to retain control over information release (Bergeron, 2000).

Security is entwined in location awareness systems because location will affect the modes of interaction between user and application. Location awareness can also affect the way in which a mobile application operates. A change in location often involves a shift in network domains, bandwidth fluctuations and bandwidth. In a world of wireless *ad hoc* networks, communications from mobile clients to network base stations are through a series of hand off processes, leaping through various domains. As wireless and mobile networks operate on a series of units called base stations (or cells or access points), each of these units has a limited geographical coverage and cell capacity. Naturally in a mobile network, cell capacity and coverage would be greater then that compared to an office 802.11 Wireless LAN. This is simply due to higher user density and market proliferation of cellular phones. However, with the introduction of Metropolitan wide wireless services such as the Metricom Ricochet, public wireless data networks will soon become the norm. In this paper, we will assume the use of a metropolitan network system and an internal office wireless network. These networks systems are integrated and interoperable as overlaying networks whereby handoffs between different networks are seamless (Stemm and Katz, 1996). It may begin as an office 802.11b network, progressing to public WANS and Metropolitan size MANS. A user may be able to cross various overlaying networks (via a series of handoffs), starting work from an internal office LAN, commuting in a public train using the Public WAN network or telecommuting on an Interstate train using the MAN.

The potential for malicious attacks on wireless clients increases if an attacker takes over or compromises the integrity of a base station. Moreover, because mobile clients wander through mobile nodes, a user might unwittingly wander into a rogue zone, set up by the

attacker. Lastly, a wireless network is an ideal springboard for an attacker to launch 'ambush' style attacks. This is because of the nature of the wireless medium, whereby the users are able to roam in and out of zones easily thereby making tracing difficult, and escaping an easy task. Hence, defining trustworthiness on the physical location of a client on the network, and which server or domain it is connected to, is equally critical in ensuring safe data transfer.

A security conscious adaptive system or mobile application must understand and consider the following contexts:

1. Physical environment where the data is sent or received. This implies places such as for example, within an office building, or outside by the train station.
2. Network space (domain) in which the mobile device is operating. The actual network itself from which the mobile client is currently hooked on.
3. The 'critical' link between the wireless client and its intended server recipient. This is the wireless link between a mobile client and it's nearest base station or access point.
4. Availability of resources to enforce security (hardware constraints, network security services)
5. The preference of the user. Users must not only be able to control the operation and use of the mobile client, but the type of information that is released to external sources.
6. Balance and identify the tradeoffs between security, location and amount of resources available to the mobile client.

Four likely scenarios that could occur in a Location Adaptive system include:

1. Mobile client is in internal LAN and wants to connect to external host. The client is within an office LAN and wants to make a connection to an external host.
2. Mobile client is in internal LAN wants to connect to internal host. The client is within the office LAN and wants to make an internal connection.
3. Mobile client is in external LAN wants to connect to external host. The client is on an external network and wants a connection to an external network or host.
4. Mobile client is in external LAN wants to connect to internal host. The client is on a public network and wants to make a connection to the user's office network.

Location Adaptive Scenarios involving Privacy and Security

Current approaches to security in location-based services (LBS) and Global Positioning Systems (GPS) have mostly centred on privacy issues. A widely known privacy concern with LBS is discussed in (Levijoki, 1998), whereby sending of information to the user is done without his or her consent. This is similar to Internet pop-up banner ads and spam. There is also worry that GPS location tracking systems infringe on the working environment and have raised ethical issues for employers using such systems employee monitoring (Levijoki, 1998). Proximity awareness, is another concern for users because, devices such as PDAs automatically exchange information (without prior notification to the user) with other devices in the near vicinity. This is a particular worry with omnidirectional *ad hoc* networks such as Bluetooth piconets. Finally, in enterprise or organisational environment**,** privacy issues begin to fall heavily into the boundaries of access control lists. BlueLocator (Chen *et al.*, 2002) describes an application that ensures privacy control over an LBS system. Other related context aware security work is mentioned by Kindberg and Kanzhang (2002). Examples cited include the use of a subject's context characteristics to establish authentication and identification. The use of location is an example of such a context characteristic used in context authentication. For example, a company computer ceases to function if not used within the confines of the office LAN. Alternatively, terminals outside a twenty-meter sphere of influence cannot access a department's laser printers.

The premise of using location adaptive systems that act based on location can be applied to today's increasingly mobile-active workforce. Several scenarios are described below, with some describing a security level escalation or de-escalation. Some of these scenarios also incorporate privacy issues.

1. A salesman, out on the field, with a GPRS phone and PDA will only have a moderately fast wireless link back to the company's inventory database. However, because the location and circumstances of his access requires a secure tunnelling into the office LAN, an adaptive security system can employ or recommend (to the user) a lower encryption bit rate should resources not permit. Similarly, if a faster network is available and hardware/ software capabilities increase, stronger encryption or security enforcement can be employed.
2. A 'location adaptive briefcase' that promptly encrypts its combination access password once the owner leaves the home with it. A sensor on the briefcase detects, that it is physically leaving the confines of a 'home zone' and initiates security measures by encrypting its password combination and locking itself.
3. Another example illustrates the case of a notebook that lowers its personal firewall because it senses that it is within the protection of the organisation's LAN firewalls and Intrusion Detection Systems. By using less security on the client itself, it's battery and CPU resources increase.
4. This example illustrates using a profile-based system to prevent unwanted push ads often associated with Location Based Systems. A user (such as a phone or PDA) has his or her profile stored on the mobile device. This profile may describe items such as the users' interests, hobbies, gender, age and a number of other descriptions, which the user enters. An LBS 'push' advertising service within proximity of the mobile device retrieves the user's profile description and tailors personalised content (e.g. sending sports sales catalogues of a nearby store, because the user lists down Tennis as one of the hobbies in the profile). This profile can be sent out automatically by the mobile device or through a proximity querying system that retrieves the profile from the device itself. This scenario also suggests privacy infringements, as a user might not like to have 'push' ads sent to him or her. However, such an approach may be also useful to a user who wants to filter out unwanted or irrelevant ads. An example of such a profile is illustrated below as Figure 2.

```
<user-profile name = John>
<name>John Smith</name>
<gender>male</gender>
<age>24</age>
<hobbies>
        <descriptor1>Tennis</descriptor1>
        <descriptor2>Cars</descriptor2>
        <descriptor3>Computer Software</descriptor3>
        <descriptor4>Reading</descriptor4>
<hobbies/>
</user-profile>
```

Figure 2: An XML based user-profile for context aware LBS systems.

5. In an LBS based m-Commerce or enterprise application scenario, privacy restrictions or information release policies can be set as profiles that are dependent on context and/ or location. This way, a user might be able to define privacy policies when he or she is at a certain location, and a different set of rules somewhere else (Snekkenes, 2001). For example, browsing through a bookstore, John's privacy profile allows a fair amount of 'push advertising' to his mobile device. The latest books and updates that correspond to his reading genre and profile are 'beamed' to his device. In addition, some information about himself is released or exchanged between the bookstore's servers, allowing a personalised portal of his book purchase history and interests. However, in a

shopping mall, information release is restricted to prevent a 'deluge' of content from flooding his device. Such a scenario is an extension the one described previously, whereby now consent and control is managed by the user.

In this paper, we have discussed privacy and security as subsets or components or each other. Privacy requires security as an enabler, however, more often then not, security is more a technical issue whereas privacy remains a social issue. The important to note however, is that privacy can be presented as an aspect of security, if the latter is implemented correctly properly. Despite this, privacy can also be viewed as a security policy that can be available to a user when at only limited times. This might come about because of resource constraints by mobile networks or devices. In general, an application can restrict privacy if the environmental context or security policies allow. Less privacy might lead to fewer resources to consume. This might be in the application of browser filters or using anonymising proxies to prevent eavesdropping. As always, providing that perfect privacy, might not be entirely possible while doing a balancing act between resources, functionality and efficiency (Kotz *et al.*, 2000). The following section describe LOCAS and its initial implementation stages, the eventual aim of LOCAS is to provide user-controllable based on Location, Security policies and Resources.

RESOURCE CONSTRAINTS IN LOCATION AWARE SECURITY

In a pervasive computing environment, it is possible that different and diverse security levels can be encountered when roaming between different domains. However, the ability for adapting to individual security policies and demands of individual domains remains a significant challenge for any mobile application to handle. Moreover, a mobile application must consider other related costs in deciding to do the adaptation of security. An excessive and general security lockdown on resource constraint devices (e.g. limited battery power, bandwidth and frequent disconnections) may require too many resources (Roman *et al.*, 2000). However, an open system where resources are not used extensively may result in a security compromise and probably a loss in privacy.

Our approach investigates the possibility of labelling defined networks or domains into "Trusted Zones" and "Untrusted Zones". It discusses the problems associated with incurring high resource overheads when attempting to enforce a multi-level security system for LOCAS.

"Trusted Zones" can be generally categorised as networks that are enforced with firewalls, have web servers that support SSL (40 or 128bit), an Intrusion Detection System, anti-virus scanners and VPN links (for secure tunnelling). Typically, organisational wide WANS or office LANS support some of the abovementioned features at the very least. An "Untrusted Zone" however, is more often a public network, or a wireless 'hotspot' zone where policy enforcement or networking security is less imposed.

In a resource-limited environment, it might not be always to use the highest level of security on mobile applications. An adaptive system has to 'make do' with any resources, it can use, while varying security accordingly to ensure optimal resource usage. Therefore, instead of simple a 'yes' or 'no' process, the use of a location aware security system hopes to achieve this feat through various degrees of granularity. Figure 3 below demonstrates a common roaming situation whereby users could continue computing activity within the secure confines of the office LAN and the 'openness' of a public operation; whereby drive-by over-the-air hack attempts can be easily conducted. By being location aware and security conscious, knowing the physical environment in which you are presently residing in can help determine the measures that need to be taken.

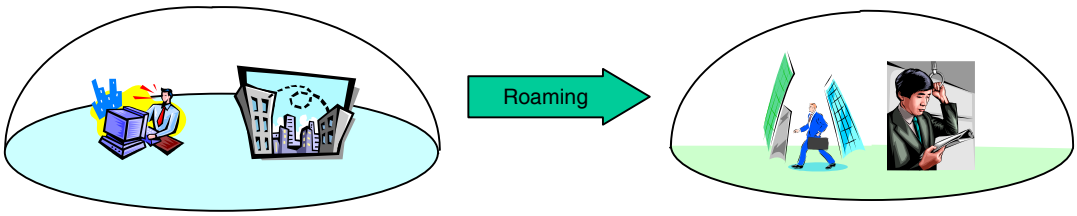

Figure 3: Roaming between zones with location awareness

Internet Security is mandatory especially since the latter is essentially a large distributed public network. However, because the mobile environment is often fraught with constraints, designing secure mobile applications is a challenge in itself. In such circumstances, a mobile client needs to optimise its resource usage. Information security appears to impose an 'all or nothing' policy, when providing a client server solution, however the key issue we want to stress in this paper is "some security (in the face of limited resources or constraints) is still better then having none at all" (Ng and Zaslavsky, 2002). What little security that can be provided under reasonable load to the client and system could offer a level of defence against most security threats. With location and resources being monitored carefully, security defence levels can be escalated and varied accordingly. Furthermore, the use of security protocols such as SSL would ensure a secure means of transmission for mobile devices. Besides SSL, use of lightweight encryption algorithms could allow security over modest bandwidth solutions.

Usage of security protocols such as SSL and encryption/ decryption processes is known to be processor intensive on thin clients such as Pocket PCs and Palm OS PDAs. Furthermore, a weak quality of service or low bandwidth link is detrimental in to the process of encryption and decryption of data. However, Gupta and Gupta (2001) point out a number of interesting insights that may provide alleviation. In the event of a slow network, "some constraints ease other", a CPU does not necessarily have to be very fast to perform bulk encryption and authentication. Because the network is already slow, the CPU does not have to decrypt and encrypting data quickly in a bid to play 'catch up' with network speeds. This would therefore ease the problems of a high CPU load. Furthermore, a standard SSL client only needs to perform public key operations instead of private key operations for signature verifications and encryption. Usage of SSL's session reuse feature also permits multiple connections without having to perform public key RSA operations repeatedly. Figure 4 illustrates a scene where a mobile user switches between different networks. Moreover, in doing so, he is faced with a range of issues that include security, location, browser and power levels.

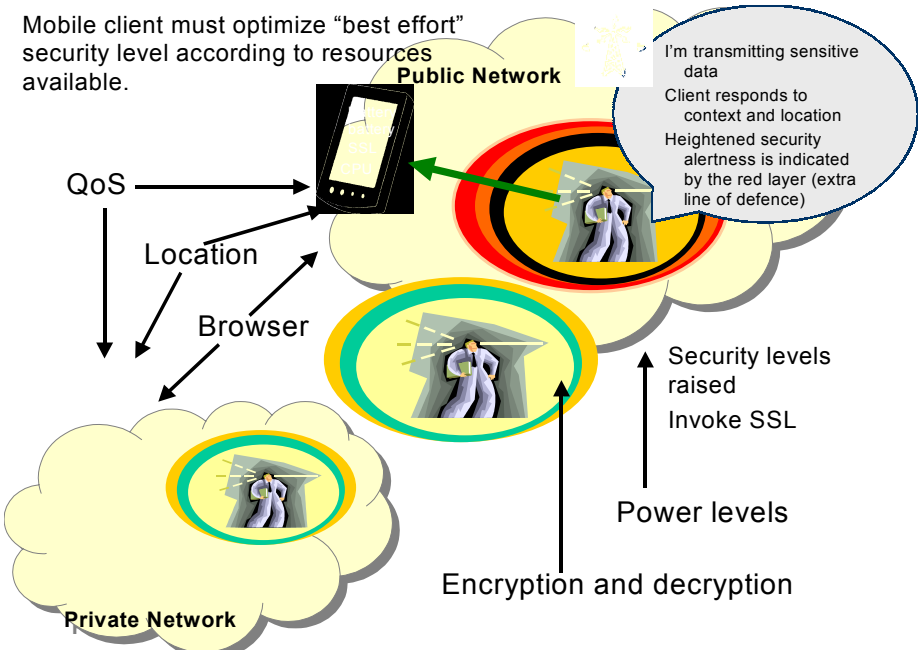

Figure 4: Roaming between 'Trusted' and 'Untrusted' networks depicting changes in Security and Context

However, in enforcing varying security levels according to the device's location and Zones, a device must consider the drain caused by using more resource intense processes. A device must also decide if where it resides warrants the need for using security. Adapting security to location and context aware parameters is a delicate balancing act that requires fine-tuning and policy implementation. Figure 5 depicts a graphical example of resource balancing as devices cross between networks and Trusted or Untrusted Zones.

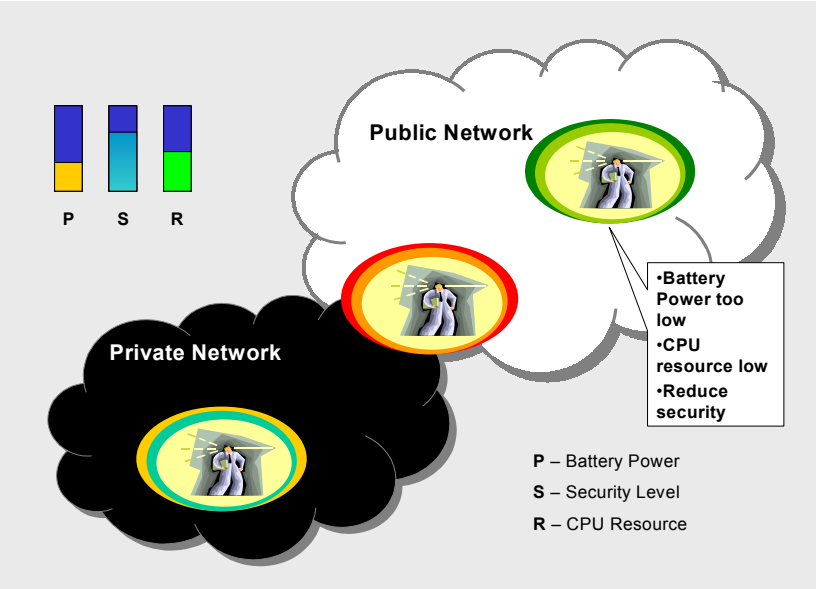

Figure 5: Resource balancing in Location Aware Security

CONCLUSION

With today's rapid rise in mobile device penetration and increased demand for data services, context awareness and location-based services will play an important role in pervasive computing. In this paper, we have approached and discussed the impact location has on security, resources and privacy (in a pervasive environment), via two different angles. This is especially meaningful in an m-Commerce scenario where privacy and security is used with discretion. Furthermore, the seemingly interconnected relationship between location, security and context awareness is a delicate balance maintained by a mobile client in a limited resource environment.

As a proof of concept, we are developing a LOCAS prototype to simulate location awareness and security under varying resource levels. LOCAS seeks to demonstrate the ability for a client to adopt a 'best effort security posture' when necessary, even in the face of resource constraint. As part of our ongoing research, we intend to plug-in privacy modules to LOCAS thereby allowing privacy restriction simulations under context aware scenarios. These privacy modules should be able to render users 'anonymous', give the option of privacy and anonymity when resources are available. These modules should also be able to dispense advice or recommendations with regards to privacy policies and options in the current network.

ACKNOWLEDGEMENTS

We appreciate and thank Ted McFadden at CRC DSTC Pty Ltd, for invaluable feedback, comments and discussion. We also would like to thank the reviewers at ACIS 2002 for comments and suggestions provided.

REFERENCES

Bergeron E, (2000) "The Difference Between Security and Privacy", Zero-Knowledge Systems Inc. Joint Workshop on Mobile Web Privacy WAP Forum & World Wide Web Consortium 7-8 Dec 2000, Munich Germany, http://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html

Chen, G and Kotz, D. (1999) "A survey of Context-Aware Mobile Computing Research", Department of Computer Science, Dartmouth College, Dartmouth Computer Science Technical Report TR2000-381 pp 1-3, pp 12.

Chen, Y; Chen, X; Ding, X; Rao, F; Liu, D. (2002) “BlueLocator: Enabling Enterprise Location-Based Services”, IBM China Research Lab, Beijing, Mobile Data Management 2002 Singapore, pp1-3.

Ghosh, A K; Swaminath T M. (2001) “Software Security and Privacy Risks in Mobile E-Commerce”, Communications of the ACM Feb 2001/Vol44 No.2 pp52-53

Gupta, V; Gupta, S. (2001) “Securing the Wireless Internet”. IEEE Communications Magazine Dec 2001 pp71-72.

Kindberg, T; Zhang, K. (2002) “Context Authentication using Constrained Channels”, Internet and Mobile Systems Laboratory, HP Laboratories Palo Alto April, pp1-2.

Levijoki, S. (1998) “Privacy vs. Location Awareness”, Helsinki University of Technology Dept of Computer Science. (http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm)

Lubinski A, (1998) “Security Adaptation Components for Mobile Computing”, Proc. of the EUROSEC’98, Paris, March 1998.

Mandato D; Kovacs E; Hohl F and Alikhani H. (2002) “CAMP: Context Aware Mobile Portal”, IEEE Communications Magazine January 2002, pp 2-4

Ng A; Zaslavsky A. (2002) “Location Awareness and Adaptable Multilayer Security in Enterprise Applications”, accepted for M-Business 2002 Greece

“Privacy Fundamentals”, Privacillia.org, http://www.privacilla.org/fundamentals/security.html

Robinson T. (2000) “Location is everything”, InternetWeek.com, Tuesday Sept 12, 2000, http://www.internetwk.com/lead/091200.htm

Roman, G.C; Picco, G; Murphy, A. (2000) “Software Engineering for Mobility: A Roadmap”, Dept Of Computer Science, University Of Maryland, Pp247-24.

Schilit B, Adams N, Want R (1994): “Context-aware Computing Applications”, proceedings of IEEE workshop on Mobile Computing Systems and Applications, pages 85-90, Dec 1994 IEEE Press.

Snekkenes E. (2001) “Concepts for Personal Location Privacy Policies”, Norwegian Computing Center, Third ACM Conference on Electronic Commerce, Tampa Florida 2001, pp1-2

Stemm, M; Katz, R. (1996) “Vertical Handoffs in Wireless Overlay Networks”. Department of Computer Science and Engineering University of California, Berkeley (1996).

Varadharajan V and Yi M (1996) “Design of Secure End-to-End Protocols for Mobile Systems”, Proc. Of the IFIP World Conference on Mobile Communications, Canberra 1996

COPYRIGHT