Survey on Location Privacy in Pervasive Computing

Andreas Görlach, Andreas Heinemann, and Wesley W. Terpstra

Darmstadt University of Technology (TUD),
Department of Computer Science,
D-64283 Darmstadt, Germany,
{goerlach,terpstra}@ito.tu-darmstadt.de, aheine@gkec.tu-darmstadt.de

Abstract. The goal of ubiquitous computing research is refine devices to the point where their use is transparent. For many applications with mobile devices, transparent operation requires that the device be location-aware. Unfortunately, the location of an individual can be used to infer highly private information. Hence, these devices must be carefully designed, lest they become a ubiquitous surveillance system.
This paper overviews existing location-sensing mobile devices, vectors for a privacy invasion, and proposed solutions. Particular attention is paid to required infrastructure and the accuracy of the location information which can be stolen. Solutions are examined from the perspective of attacks which can be reasonably expected against these systems.

1 Introduction

The proliferation of portable electronic devices into our day-to-day lives introduced many unresolved privacy concerns. The principle concern in this paper is that these devices are being increasingly equipped with communication capabilities and location awareness. While these features present a wide array of new quality-of-life enhancing applications, they also present new threats. We must be careful that the potential quality-of-life lost through the surrender of private information does not overwhelm the benefits.

An important question is how much privacy protection is necessary. Perfect privacy is clearly impossible as long as communication takes place. Therefore, research aims at minimizing the information disclosed. The required level of this protection is not a matter of technology; different people have different privacy needs. Nevertheless, technology should not *force* society to accept less privacy.

The major privacy concern with mobile devices equipped with communications ability is that they can reveal the location of their bearers. This concern is in itself not new; people can recognize each other. What is new is the increased scope of the problem due to automated information gathering and analysis. Poorly designed mobile devices enable anyone to obtain another's location.

If we allow automation to create an effective public record of people's locations, discrimination against minorities will be impossible to control. AIDS

patients could be identified by the offices of doctors they visit, Alcoholics Anonymous members by their group meetings, and religious groups by their churches.

This paper will present an overview of the state-of-the-art in location privacy. In Section 2, mobile devices which possess both location awareness and communication ability will be examined. Section 3 lists attacks by which an invader can obtain your private location information. Existing countermeasures and safeguards are detailed in Section 4. These include high level schemes such as policies which operate like contracts, and lower-level solutions which reduce information disclosure. Among the latter are anonymous routing algorithms, schemes for hiding within a group, methods to passively determine location, and frequency modulation techniques to hinder triangulation.

2 Location-Aware Communication Devices

Many technologies can determine the location of an individual. This section provides an overview of what technologies are presently deployed and which are coming in the near future.

One of the earliest systems designed for location tracking is the Global Positioning System (GPS) [10]. This system uses satellites to help devices determine their location. The GPS works best outdoors where it has line-of-sight to the satellites and few obstructions. For commercial products, resolution to within 4m is achievable. The GPS is widely deployed and integrated, especially in map applications. Although GPS devices do not transmit, they are being increasing integrated into PDAs and other devices which do.

For indoor use, the Active Badges[21] from AT&T Laboratories Cambridge were developed. These are small devices worn by individuals which actively transmit an identifier via infrared. This information is received by sensors deployed in the environment. This system provides essentially room-level resolution and has problems following individuals due to the infrequency of updates. The environment consolidates this information and can provide the current location of an individual.

A later refinement, the Bat[22], increased the detected resolution. With the increased resolution, the Bat can be used to touch virtual hot spots. Their work reports accuracy as good as 4cm. These refined devices used ultrasonic pings similar to bat sonar. However, once again the environment measures the Bat's location as opposed to real bats which learn about their environment.

The Cricket Location-Support System[17] system takes a similar approach. It uses radio and ultrasonic waves to determine distance and thus location. Like the Cambridge Bat, resolution to within inches is possible. As opposed to the similar Cambridge work, beacons are placed in the environment as opposed to on individuals. The Cricket devices carried by individuals listen to their environment in order to determine their location. In this way, the device knows its location, while the environment does not.

An approach to location sensing which does not require new infrastructure is taken by Carnegie Mellon University [19]. Here, the existing wireless LAN is

observed by devices to recognize their location. By passively observing the signal strengths of various base stations, a device can determine it's location. Though there are no requirements for new infrastructure, there is a training overhead. During training a virtual map of signals is created which is used by the devices to determine their location.

Cell phones can be abused to provide location information. Although not originally intended for this purpose, the E-911 [18] requirements in the US forced cell phone providers to determine customer location when they dialed an emergency phone number. Although this practice was clearly beneficial, the technology has since spread. The underlying problem is the omnipresent possibility of performing triangulation (with varying accuracy, though).

In the near future Radio Frequency Identification (RFID) [9] will be found in many consumer goods. Intended as a replacement for barcodes, these tiny devices are placed in products to respond to a wireless query. Unlike barcodes, RFIDs are distinct for every item, even those from the same product line. This allows companies to determine their inventory by simply walking through the shelves and automatically recording the observed products.

3 Attacks on Location Privacy

In a successful privacy attack, some party obtains unauthorized information. Individuals intend that some informations about themselves should be available to others, and that the rest remain private. The means by which the individual's preferences were circumvented is the attack vector.

The main privacy concern with regards to ubiquitous computing is that many new *automated* attack vectors become possible. Loosely categorized, automated digital devices obtain information either through communication, observation, or inference. In this section the attack vectors available in each of these channels will be explored.

3.1 First-Hand Communication

An attacker obtains private information through first-hand communication when an individual unwittingly provides it directly to the attacker. In a world with ubiquitous computing, the threat of disclosure via accident or trickery is significant. All digital devices of a given type, by virtue of being homogeneous, make the same mistakes—and don't learn from them. The designers of the Windows file sharing protocol never intended it to be used to obtain people's names. Nevertheless, Windows laptops will happily reveal their owner's name to anyone who asks it. Due to a bug in bluetooth phones, attackers may often trick the phone into revealing its address book and phone number[16]. By asking a device with known location for owner information, both of these attacks pinpoint the owner's location, among other things. Naturally, these attacks can be built into an automated device.

Many ubiquitous devices also exhibit drunken behaviour. The Bats and Active Badges broadcast their location information for all to hear. WLAN cards periodically emit traffic which includes their unique MAC ID. Devices providing exact their location information to location based services also seems overly permissive. At the bare minimum, these problems must be addressed.

A unique characteristic of digital devices is their potential for brain-washing. Manufacturers may choose to place secret spyware in their products[1] as a means to recoup financial losses. Furthermore, a vulnerability may allow an attacker to completely assume control of the device, and thus obtain a live location feed. For devices where the location information is known to the infrastructure, the threat of a system vulnerability is magnified.

3.2 Second-Hand Communication

Also known as gossip, attacks via second-hand communication relay information from one party to another unauthorized party. The primary difference between these attacks and first-hand attacks is that the individual no longer controls the information. Fortunately, in the human scenario, talking about individuals behind their back requires some expenditure of breath. Unfortunately, aggregation and spreading of this information in a digital system is significantly easier.

This behaviour has already been observed in the Internet where Doubleclick regularly sells personal habit and preference information. It seems naïve to assume that the much finer grained information available from ubiquitous devices will not similarly be sold. Services are already available for individuals to locate their friends via the cell phone networks[1].

3.3 Observation

Attackers may also obtain information by configuring devices to observe their environment. The most obvious problem is the deployment of many nearly-invisible cameras in the environment. However, there are other risks which are more feasible to launch with current technology.

One of the more interesting attacks that can be launched against mobile communications-equipped devices is triangulation. By measuring timing delays in a signal, the attacker can determine the location of the device. This is similar to how the Bat operates, only using electromagnetic waves instead of sound waves.

3.4 Inference

One of the fears about automated privacy invasion is the compilation of a profile. After gathering large amounts of information via communication and observation, an automated system combines these facts and draws inferences. Given enough data, the idea is to build a complete picture of the victim's life.

[1] For example the Kazaa Media Desktop

From a more location-centric point of view, location information could be processed to obtain useful information for discrimination. If a person regularly visits the location of a group meeting, she is probably a member of that group. In the consumer arena, the fact that an individual shops at a particular store at regular intervals may be useful information for price discrimination[2].

Tracking an individual's location through time may also enable an attacker to link information to the individual. For example, if an individual's car regularly sends out *totally anonymous* weather requests, it might still be possible for a weather network to track the car by correlating the observed request locations. Later, when the individual buys gas at an affiliate's gas station, the network can link the individual's name and bank account to the tracked car. Now, the network can deduce information such as where the person shops, lives, and works; who the person regularly visits; etc.

4 Solutions

In the literature there exist several approaches to protect the location of a user. Most of them try to prevent disclosure of unnecessary information. Here one explicitly or implicitly controls what information is given to whom, and when. For the purposes of this paper, this information is primarily the identity and the location of an individual. However, other properties of an individual such as interests, behaviour, or communication patterns could lead to the identity and location by inference or statistical analysis.

In some cases giving out information can not be avoided. This can be a threat to personal privacy if an adversary is able to access different sources and link the retrieved data. Unwanted personal profiles may be the result. To prevent this, people request that their information be treated confidentially. For the automated world of databases and data mining, researchers developed policy schemes. These may enable adequate privacy protection, although they similarly rely on laws or goodwill of third parties.

4.1 Policies

In general, all policy based approaches must trust the system. If the systems betrays a user, his privacy might be lost. Here, the suitable counter-measure is a non-technical one. With the help of legislation the privacy policy can be enforced.

All policy based systems have the drawback that a service could simply ignore the individual's privacy preferences and say, "To use this service you have to give up your privacy or go away." This certainly puts the user in a dilemma and he will probably accept these terms as he wants to use the service.

A Privacy Awareness System (pawS) for Ubiquitous Computing Environments In [14, 15] Langheinrich proposes the *pawS* system. *pawS* provides

users with a privacy *enabling* technology. This approach is based on the Platform for Privacy Preferences Project (P3P) [5], a framework which enables the encoding of privacy policies into machine-readable XML. Using a trusted device, the user negotiates his privacy preferences with the UbiCom environment.

Framework for Security and Privacy in Automotive Telematics A framework for security and privacy in automotive telematics, i.e. embedded computing and telecommunication technology for vehicles, is described by Duri *et al.* [6]. The primary goal of their framework is to enable building telematics computing platforms that can be trusted by users and service providers. They do that by installing a *data protection manager* to handle sensitive data. Thus they implement a middleware working with different key concepts which for example influence location data accuracy and enable user defined privacy policies.

Concepts for Personal Location Privacy Policies Snekkens [20] presents concepts which may be useful when constructing tools to enable individuals to formulate a personal location privacy policy. Snekkens's idea is that the individual should be able to adjust the accuracy of his location, identity, time, and speed and therefore have the power to enforce the need-to-know principle. The accuracy is dependent on the intended use of the data, and the use in turn is encoded within privacy policies.

4.2 Protecting First-Hand Communication

Most approaches address the problem of information disclosure. Many different ideas have been proposed to prevent unnecessary information from becoming known to a third party.

ANODR: ANonymous On Demand Routing With the scenario of a battlefield in mind, Kong and Hong described in [13] their scheme ANDOR. This is a routing protocol addressing the problems of route anonymity and location privacy.

The intention is that packets in the network can not be traced by any observing adversary. Additionally, their routing scheme provides unlinkability. Prior to one node's ability to send a message to another, a route must be established through route discovery. This route discovery is achieved by broadcasting and forwarding packets. The sender of a message is anonymous because it is impossible to judge whether a node is actually sending a message it generated or is simply forwarding a packet as part of a route.

MIXes in Mobile Communication Systems It is easy for cellular networks like GSM to track their mobile subscribers. Location information is required in order to route calls appropriately. Avoiding this by simply broadcasting is not an option because of the limited bandwidth in current cellular networks. In [7] this is investigated and the application of MIXes (see also [4]) is proposed.

In their system, the scheme does not keep the identity—telephone number—of the recipient anonymous. Only the location of the recipient is protected. Remarkably, their system remains secure even if *all* of forwarding nodes are observed by an adversary.

Mix Zones A recent approach which is somewhat similar to mix networks is *mix zones*[3]. In these networks, the infrastructure provides an anonymity service. The infrastructure delays and reorders messages from subscribers within a mix zone to confuse an observer.

A problem with this system is that there must be enough subscribers in the mix zone to provide an acceptable level of anonymity. Beresford and Stajano conducted statistical attacks against these systems and found the afforded security to be quite low. Even large groups using the Active Bat remained vulnerable.

Temporal and Spatial Cloaking In [11], Gruteser and Grunwald propose a mechanism called *cloaking* that conceals a user within a group of k people. They consider a user as *k-anonymous* if, and only if, they are indistinguishable from at least $k-1$ other users. To achieve this, the accuracy of the disclosed location is reduced. Then any of the people within the disclosed area could have been the user. Similarly, they consider reducing the accuracy of disclosure timestamps. Like Stajano and Beresford they, too, measured anonymity in experimental setups, but unlike them Gruteser and Grundwald identified concrete values which in their view provide certain levels of anonymity.

The Cricket Location-Support System In order to prevent the potential misuse of personal information, the most convincing solution is to not let out any information at all. This idea is applied directly to the Cricket Location-Support System[17]. As described in section 2, the mobile device never transmits at all; rather, it passively listens to its environment.

This system is ideally suited to an office. The transmitters need not be connected to each other or a network. This not only supports privacy, but also makes things cheaper and more maintainable. However, the use of services sometimes makes it necessary for the device to disclose its location. For example, using a printer implicitly reveals that the device is near to the printer.

The Blocker Tag A special case among pervasive devices are RFIDs. People carrying objects which contain RFIDs might not even be aware of the existence of these devices because of their size[2] and their passive nature. A second specific property of RFIDs is their unability to do any computation like e.g. encryption. So they require their own measures for privacy protection.

Juels, Rivest and Szydlo examined several possible solutions in [12] ranging from destruction of the tag through less destructive approaches to regulation (i.e. policies). Since the authors see disadvantages in all of the examined solutions they present their own approach which is the development of a special tag: the

[2] The smallest RFIDs are currently only of 0.4mm * 0.4mm size.

Blocker Tag. This tag blocks attempts of readers to identify RFIDs. In order not to block desired RFIDs or to temporarily enable the reading of RFIDs the blocking process can be done selectively.

Hindering Triangulation As mentioned in Section 3.3, data can be gathered by observing a device or person. On the physical layer it is usually possible to locate a sending device by recording signal delays and performing triangulation.

In [8] frequency modulation schemes are discussed to prevent location of mobile devices. The researchers performed an in-depth analysis of direct sequence spread spectrum. Their idea is to make it difficult to distinguish a signal from random background noise. This is done by distributing the data on pseudorandomly chosen channels. By knowing a shared secret the supposed receiver is able to reassamble the messages. The drawback of this solution is that it requires existing infrastructure to be changed and consumes considerably more bandwidth.

5 Conclusions

The solutions we have seen can be categorized into policies and information minimizing at the source. These approaches aim to address threats in the areas of first- and second-hand communication, observation, and inference.

Policies seem to work well wherever consent underlies the transaction. For example, when information is to be provided to a service, an agreement can be reached regarding the further distribution of the information. If no agreement can be reached, then the individual will be unwilling to use the service, but the service will likewise not obtain the information or any associated remunerate. Similarly, the individual can negotiate terms about how his information may be used; this can address attacks based on inference.

There is no consent in observation. This means that policies can not be applied to these attacks since the individual is in no position to negotiate. Here, legal safeguards and countermeasures are required. Unfortunately, there is currently insufficient discourse between technical and legal experts.

Accuracy reduction techniques apply primarily to first-hand communication problems. These schemes aim at reducing the amount of confidential information disclosed to third parties. There are a variety of techniques which obscure the location information, the timestamp of the transaction, and the identity of the individual.

As mentioned in the introduction, privacy issues are fundamentally not technical. As ubiquitous devices permeate the every-day lives of ordinary citizens, our privacy protection measures will have increasing impact on their lives. It is important that research into privacy protection bear in mind what must be protected. This is more the area of social sciences, and thus requires more interdisciplinary discourse.

6 Acknowledgements

This work was sponsored in part by the Deutsche Forschungsgemeinschaft (DFG) as part of the PhD program "Enabling Technologies for Electronic Commerce".

References

1. Mobiloco - Location Based Services for Mobile Communities. `http://www.mobiloco.de/`.
2. J. Bailey. Internet Price Discrimination: Self-Regulation, Public Policy, and Global Electronic Commerce, 1998.
3. A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *PERVASIVE computing, IEEE CS and IEEE Communications Society*, (1):46–55, 2003.
4. D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
5. L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. `http://www.w3.org/TR/P3P/`, seen 2004.
6. S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang. Framework for Security and Privacy in Automotive Telematics. In *International Conference on Mobile Computing and Networking*, pages 25–32. ACM Press, 2002.
7. H. Federrath, A. Jerichow, and A. Pfitzmann. MIXes in Mobile Communication Systems: Location Management with Privacy. In *Information Hiding*, pages 121–135, 1996.
8. H. Federrath and J. Thees. Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern. *Datenschutz und Datensicherung, Verlag Vieweg, Wiesbaden*, 6(6):338–348, 1995.
9. K. Finkenzeller. *RFID-Handbook, 2nd Edition*. Wiley & Sons LTD, 2003.
10. I. A. Getting. The Global Positioning System. *IEEE Spectrum*, 30(12):36–47, December 1993.
11. M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys*, pages 31–42. USENIX, 2003.
12. A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *V. Atluri, ed. 8th ACM Conference on Computer and Communications Security*, pages 103–111. ACM Press, 2003.
13. J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 291–302. ACM Press, 2003.
14. M. Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In G. D. Abowd, B. Brumitt, and S. A. Shafer, editors, *Ubicomp*, volume 2201 of *Lecture Notes in Computer Science*, pages 273–291. Springer, 2001.
15. M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In G. Borriello and L. E. Holmquist, editors, *Ubicomp*, volume 2498 of *Lecture Notes in Computer Science*, pages 237–245. Springer, 2002.
16. A. Laurie. Serious Flaws in Bluetooth Security Lead to Disclosure of Personal Data. `http://www.bluestumbler.org`, 2003.

17. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket Location-Support System. In *Mobile Computing and Networking*, pages 32–43, 2000.
18. J. H. Reed, K. J. Krizman, B. D. Woerner, and T. S. Rappaport. An Overview of the Challenges and Progress in Meeting the E–911 Requirement for Location Service. *IEEE Communications Magazine*, 5(3):30–37, April 1998.
19. A. Smailagic, D. P. Siewiorek, J. Anhalt, D. Kogan, and Y. Wang. Location Sensing and Privacy in a Context Aware Computing Environment. In *Pervasive Computing*, 2001.
20. E. Snekkenes. Concepts for Personal Location Privacy Policies. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pages 48–57. ACM Press, 2001.
21. R. Want, A. Hopper, V. Falcão, and J. Gibbons. The Active Badge Location System. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.
22. A. Ward, A. Jones, and A. Hopper. A New Location Technique for the Active Office. *IEEE Personal Communication*, 4(5):42–47, 1997.