Security & Privacy in a World of Pervasive Computing

UNIVERSITY OF BATH

DEPARTMENT OF COMPUTER SCIENCE: CS50200
CANDIDATE NUMBER: 02151
4/12/2017

Pervasive computing is becoming a cornerstone of modern society. With the increasing ubiquity of smart devices in our everyday lives, security and privacy are a real concern. In Pervasive computing security concerns with respect to privacy confidentiality, digital rights, and reliability are more human centered socially oriented concerns rather than technical ones. This puts a great deal of emphasis on the trustworthiness of the system as more human interaction is removed and sensor networks and embedded computers become the primary interaction. The goal of this paper is to understand the relationships between security, personal privacy and trust of pervasive computing systems as they act as the society-technology bridge.

Introduction

Pervasive computing was first described by IBM in 1996 as embracing the vision of computing services available anytime, anywhere and on demand [1] and again by Weiser stating that computers will become so ubiquitous that no one will notice their presence [2]. Modern advances in pervasive computing has been driven by the growth of wireless networking services and ubiquitous computing devices, both of which have helped approach the vision of a truly pervasive computing world. Combining technology and concepts from many fields such as mobile computing, wireless networking, embedded computing, context awareness, and HCI; pervasive systems can be exceptionally diverse in capabilities and functions.

Examples of pervasive computing systems can be as simple as everyday mobile devices and wearables [3] to highly complex, fully integrated computing environments known as smart spaces and adaptive environments [4] [5]. Pervasive computing has advanced to the point where their technologies are now being considered as a foundation of new constructions rather than a later addition with ambient computing being integrated directly with architecture [6]. A large majority of these systems rely on sensory input and contextual awareness to carry out their functions with limited human interaction.

Personal information is required to develop useful levels of contextual information, this leads to obvious security and privacy concerns with personal data being stored and used by these entities. The obvious weakness comes when these entities in pervasive computing are required to operate while disconnected from any home network, thus having no access to a centralised identity controlling authority. These security issues as well as potential privacy concerns will be discussed.

Security & Privacy

Influence of Context on Privacy & Security

Defined by Dey as any information that can be used to characterize the situation of an entity [7], contextual information is a powerful tool for enabling pervasive computing systems to carry out their functions with limited human input. Contextual information can vary substantially in type, ranging from location in-

formation to identifying information such as a users gender or profession. The context contributes to the meaning that a human being assigns to a communication or information. The same information exchanged can mean something entirely different in two different contexts. As such this contextual information can be used to adjust and alter an applications behaviour, which can have obvious implications on the requirements and provisions regarding privacy, security and trust.

Due to the sensitive nature of many aspects of contextual information, privacy is a key concern with most context aware systems. this is especially the case with mobile devices and other publically networked systems which are common in pervasive computing solutions. The importance of context within pervasive systems stems from the fact that all the available information is necessary to provide a useful and meaningful decision by the system in complex pervasive computing environments. This essentially means that all aspects of the system require complete access to contextual resources. Combining contextual information with the systems application data while maintaining user trust, correctly recognising the user and protecting their identity while maintaining all aspects of any specific security policy is a key challenge for pervasive environments.

This security issue is best illustrated with an example. Consider a GPS system in a car that identifies the user's location, it then looks up the user's calendar information from the users connected mobile device and compares the next appointment location to the users current location and passes the information onto the GPS application which returns the estimated time taken and a route for the user to take. This is completely autonomous and a good example of a pervasive system, in this case in a car. The contextual information here is the user's calendar schedule and their current location. This clearly requires the exchange of location information between devices. A great deal of information can be inferred if the location of a user is continuously monitored. It is often feasible to restrict the use of location information to lower levels of applications, thereby attempting to avoid revealing it unnecessarily increasing the security of the system. However, the privacy concern is much higher as users are not aware of how much personal information is collected and what the content of the context data is. As such it is often argued that in pervasive systems trust and privacy are of more concern than technical security.

Security in Pervasive Systems

The security of information can be broken down into six key categories; information availability, authenticity, authority, integrity, confidentiality, and reliability. For typical systems this information security is maintained via cryptography, security protocols, and tamper resistance. For pervasive systems, however, security needs to be scalable to the small computational resources available to most embedded computing devices but also able to deal with devices and environments of unknown origin. Another key requirement of pervasive security systems is that they must be adaptive to the dynamics of mobile computing and socially motivated security decisions.

As such specific security protocols and systems are required for each application, an example of which is RFID systems. Intended as a replacement for barcodes, RFIDs respond to wireless queries, but unlike barcodes they are distinct for each individual item rather than a product line [8]. RFID security protocols are typically based around either a "kill command" or a hash-based protocol, however, this leaves the RFID tag useless after being activated or has various cryptography related vulnerabilities [9]. Rhee1 et. al. propose an alternative security protocol specifically for RFID tags which uses a challenge-response method meaning the protocol is secure against replay and spoofing attacks which hash-based protocols can be vulnerable to [10].

Protecting user identity when contextual information is used is challenging, traditionally this is achieved using anonymizers (independent trusted mediators) however this is vulnerable to a singular point of failure. Rahman et. al. propose a methodology for contexted based applications in mobile and pervasive en-

vironments that uses a collaborative model to remove the need for an anonymizer [11]. Contextual information itself can be used within the security protocol [12] [13]. These frameworks allow or block network access and data based on the context of the user at the time of the security request. If the request by the application is considered to be unreasonable for the context of the user it is blocked. For example, a fitness application that tracks a user's speed and distance traveled over a course of a run that requests location data from the device when the user's context has been identified as sat in a work office would have this request blocked. This helps to reduce the risk of users daily personal activities being inferred from data passively collected by the application when the application is not in use. Covington et. al. propose an alternative security framework which also uses contextual information by requiring the platform to provide assurances in the security of the contextual data that is reported [14]. It achieves this by using contextual attributes to support and enhance authentication.

Protecting Privacy & Establishing Trust

Privacy requirements within pervasive computing can be broken down into the following categories:

- Purpose specification: the purpose for which the information has been collected.
- Consent: the purposes associated with the information must have the consent of the user.
- Limited collection, use, disclosure & retention: the information collected, used, disclosed and retained shall be limited to the minimum necessary.
- Accuracy: personal information stored should be kept up to date.
- Safety: Personal information must be protected by security safeguards against misuse.
- Openness: A user should have full access to their own information.

These concepts have become known as Hippocratic Databases [15]. Privacy management systems aim to maintain these principles and systems have been developed that take conventional methods of privacy protection, such as Role Based Access Control (RBAC), and adapts them for pervasive computing environments [16]. It is clear, however, that the majority of privacy concerns that arise stem from the fact that individuals are either not aware of how much personal information is collected, this directly impacts user trust and makes the majority of privacy issues less of a technical issue but more of a social one.

Due to the sensitivity of personal information that is collected by most context aware systems, user privacy and a users trust in the system can be argued as more of a concern than technical security. In computing trust is widely captured by the term trust management [17]. Trust management methodologies support descriptions on how to facilitate relationships between entities. This enables entities that are identified as trusted to exchange information without the need of an administrator to authorise the interaction. This allows users and systems to grant access to resources based on the entities trustworthiness rather than conventional authorisation techniques. These trust management systems aid in taking autonomous decisions on which entities to trust and to what degree to trust them.

In dynamic environments, such as in pervasive computing, it is clear that these interactions are established based on individual entities trustworthiness at a particular time and for a particular interaction rather than a fixed access rights policy. Various proposed systems for trust management in pervasive computing environments have been proposed. One such example is that of Secure Environments for Collaboration among Ubiquitous Roaming Entities (SECURE) which aims to apply a more human notion of trust [18]. This clearly leads to a decentralised security management approach with its obvious inherent risks. They justify this approach by stating that the ability to rea-

son about trust and risk is what lets the entities accept risk in interactions. As such they aim to form a formal basis for reasoning about trust and making decisions that are adaptable to various scenarios.

It is clear that there is an inherent opposition between privacy and trust. The more shared information the more accurate the trustworthiness assessment of an entity will be, however, the more information known by the entity the less privacy is left to the user. Seigneur and Jensen discuss this trade off in relation to a trust/risk-based security framework and the SECURE framework mentioned previously and use evidence gathering components to update risk and trust information [19].

A key aspect of building trustworthiness is correct and secure identification of entities. Xiao et. al. discuss trustworthiness and authentication of identities in pervasive and ubiquitous computing systems and reinforce the issue of the lack of a centralised authentication system which is required by conventional methods [20]. They provide a comprehensive summary of alternative, distributed, approaches to authentication in pervasive systems, touching on multi-level hierarchical trust models, local group trust models, and probability based models. Ultimately, however, they conclude that authentication of identities remains an open problem in the field of pervasive computing with no one solution putting forward a comprehensive concept of a trustworthy authentication methodology.

Conclusions

It has been identified that privacy and security in pervasive computing systems are two connected, but distinct issues. Security systems can be considered more encompassing of the technical requirements for maintaining information safeguards. Whereas privacy is managed more by trust management systems which are more dictated by the socially motivated, highly dynamic privacy requirements of mobile and public environments.

Security issues were specifically discussed, with examples drawn from RFID tags and the pros and cons of various security protocols discussed such as kill commands and hash-based protocols. The key security challenge identified was that of protecting identity when contextual information is exchanged. This was due to the highly personal nature of contextual information as well as issues with anonymisation in public systems. Solutions were presented in the forms of context aware security frameworks which look to be a promising path in forming highly dynamic security protocols needed for pervasive environments.

In regards to privacy protection, the situation is much more complex due to the majority of privacy issues stemming from the fact that users are often unaware of the information collected about them and the use of such contextual data. The requirements of Hippocratic databases were discussed as well as potential flaws in conventional privacy methodologies that occur when applied to pervasive systems. It was identified that in these highly dynamic environments that the trustworthiness of the entity at a particular time and for a particular interaction is more crucial than a fixed access rights policy. Various solutions to this were discussed, such as SECURE access policies which aim to apply human like notions of trust to computational entities. However, it is clear that there is a current lack in appropriate methodologies that accurately manage trust and privacy to abide fully by the hippocratic database outline, particularly when it comes to authentication of individual entities in the pervasive environment.

Ultimately it is concluded that, despite technical solutions existing for many potential security problems, the socially motivated requirements for privacy in pervasive environments mean no full solution exists. This leaves the problem of controlling privacy and trust in pervasive environments an open question.

References

[1] Bruce Schechter. *Seeing the light: IBM's vision of life beyond the PC.* 1999.

[2] M. Weiser. The computer for the 21st century. *Scientific American*, 265:94–104, Sep 1991.

[3] J. Hong and M. Baker. Wearable computing. *IEEE Pervasive Computing*, 13(2):7–9, Apr 2014.

[4] Jong Hyuk Park, Mohammad S. Obaidat, and Vincenzo Loia. Smart devices and spaces for pervasive computing. *Journal of Systems Architecture*, 60(8):668 – 670, 2014.

[5] Norbert Streitz Jane Siegel Volker Hartkopf Shinichi Konomi. *Cooperative Buildings. Integrating Information, Organizations, and Architecture.* Springer-Verlag, Berlin Heidelberg, 1999.

[6] S. Tzimopoulou. Urban ambient environment and sustainability. In *2011 Seventh International Conference on Intelligent Environments*, pages 245–250, July 2011.

[7] Anind K. Dey. Understanding and using context. *Personal and Ubiquitous Computing*, 5(1):4–7, Feb 2001.

[8] Klaus Finkenzeller. *RFID-Handbook.* Wiley & Sons LTD, 2nd edition, 2003.

[9] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*, pages 201–212. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[10] Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won. Challenge-response based rfid authentication protocol for distributed database environment. In Dieter HutterMarkus Ullmann, editor, *Security in Pervasive Computing*, pages 70–84, Boppard, Germany, 4 2005. Second International Conference, SPC.

[11] Farzana Rahman, Md. Endadul Hoque, and Sheikh Iqbal Ahamed. Proqupri: Towards anonymity protection with privacy quantification for context-aware applications. In *Proceedings of the 2011 ACM Symposium on Applied Computing*, SAC '11, pages 453–454, New York, NY, USA, 2011. ACM.

[12] Yaser Mowafi, Dhiah Abou-Tair, Tareq Aqarbeh, Marat Abilov, Viktor Dmitriyev, and Jorge Marx Gomez. A context-aware adaptive security framework for mobile applications. In *Proceedings of the 3rd International Conference on Context-Aware Systems and Applications*, ICCASA '14, pages 147–153, ICST, Brussels, Belgium, Belgium, 2014. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[13] Georgia M. Kapitsaki and Iakovos S. Venieris. Pcp: Privacy-aware context profile towards context-aware application development. In *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*, iiWAS '08, pages 104–110, New York, NY, USA, 2008. ACM.

[14] Deepak J. Manohar Michael J. Covington, Manoj R. Sastry. Attribute-based authentication model for dynamic mobile environments. In John A. ClarkRichard F. PaigeFiona A. C. PolackPhillip J. Brooke, editor, *Security in Pervasive Computing*, pages 227–242, York, UK, 4 2006. Third International Conference, SPC.

[15] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Chapter 14 - hippocratic databases. In Bernstein Philip A., , Ioannidis Yannis E., , Ramakrishnan Raghu, , and Papadias Dimitris, editors, {*VLDB*} *'02: Proceedings of the 28th International Conference on Very Large Databases*, pages 143 – 154. Morgan Kaufmann, San Francisco, 2002.

[16] Kyu II Kim, Won Gil Choi, Eun Ju Lee, and Ung Mo Kim. Rbac-based access control for privacy protection in pervasive environments. In *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication*, ICUIMC '09, pages 255–259, New York, NY, USA, 2009. ACM.

[17] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In *Proceedings 1996 IEEE Symposium on Security and Privacy*, pages 164–173, May 1996.

[18] V. Cahill, E. Gray, J. M. Seigneur, C. D. Jensen, Yong Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielson. Using trust for secure collaboration in uncertain environments. *IEEE Pervasive Computing*, 2(3):52–61, July 2003.

[19] Jean-Marc Seigneur and Christian Damsgaard Jensen. *Trading Privacy for Trust*, pages 93–107. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[20] Hannan Xiao, James Malcolm, Bruce Christianson, and Ying Zhang. Trustworthiness and authentication in ubiquitous computing. In *Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access*, MobiWac '12, pages 135–138, New York, NY, USA, 2012. ACM.