Privacy, Security, and Trust in Ubiquitous Computing

Introduction

The term “ubiquitous computing” first appeared in the late 1990s with a vision of computing services being available anytime, anywhere and on demand. Since then, technology advancements have been bringing society nearer to that vision with the interoperability of devices, applications, and wireless networks. The Internet of Things applies context awareness so that computers can identify the situation of the user such as location, preferences, and habits. Although it may seem like a convenience for users at first, it exposes users to potential threats in time. This leads to potential risks of privacy, security, and trust in the use of ubiquitous computing as they would not only be pervasive, but also invasive and intrusive to daily lives of users.

Due to the vast amount and large variety of information collected by different industries, pervasive computing is often described as a system of user surveillance and monitoring. In fact, recent news from CNN [9] revealed that WikiLeaks exposed the Central Intelligence Agency Code in United States hacking into smartphones and smart televisions to monitor the citizens. Considering the prediction that more Internet of Things will be embedded in the homes of people, more unwanted parties would be able to get access to information about the users under “forced” voluntary acceptance to terms and conditions of usage. This means that these devices mostly require users to allow their information to be disclosed before the service or product can be used [8]. This poses a risk towards manipulation and exploitation of consumers. The disclosure of information poses a dilemma between privacy and security as to secure one is to lose another. The balance point is then decided by the user’s trust towards the system.

The paper will first define privacy, security, and trust for an understanding of how they relate to each other. Then the paper will break apart these entities to discuss the main challenges around them and show how designers can be aware of these challenges and build better systems for users to rely on during their development processes. Besides that, the paper will give advice on how users can be aware of and deal with breaching of information.

Definitions

To discuss the main challenges, the entities of privacy, security, and trust should first be defined clearly as they are interrelated (see Figure 1). Privacy is defined as a basic right to control the collection and usage of personal information [1]. It is important because it protects an individual from being identified by unwanted parties. In contrary, security is the defence against malicious actions critical for self-protection of the system. It is important for protecting the system as well as users from negative impacts. In some cases, security also takes privacy into account to protect the identity of an individual. Compared with privacy and security, trust is the reliability of an individual towards the system. It is mediated by privacy and security, as well as being a mediator between the two entities. To put it simply, the individual’s trust towards a system changes their behaviour and attitudes towards having their information collected even without administrators to give permissions for interactions [7]. Trust itself is also evaluated by the privacy and security of the system depending on the amount of information and the extent as to the level of degree that is revealed [7].

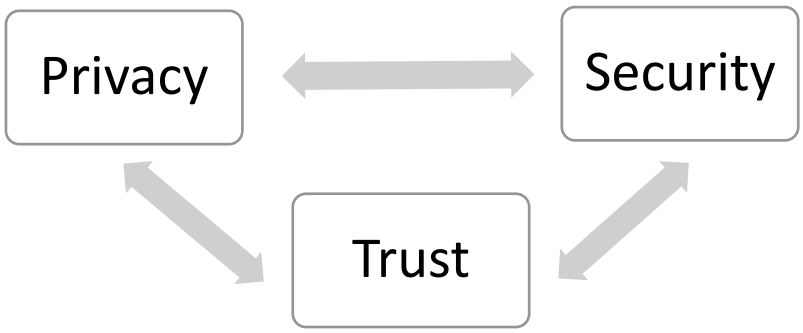

Figure 1. Interrelationship of Privacy, Security, and Trust

Privacy

The main issue with privacy is that anonymity of user data cannot be guaranteed in certain pervasive computing systems. In the United Kingdom, recent news reported that internet companies are required to retain web history of customers for a year based on the Snooper's Charter [9]. This is like giving authoritative powers permission to conduct mass surveillance within the country as they are now equipped with not just identity information from existing databases but also contextual information such as users' habits, especially when data comes from fully embedded smart homes that can give the government a sense of an entire family's situation. With a constant collection of personal details and processing of user context through wireless networks with nodes embedded in the system, it poses a serious threat of data being revealed and exchanged without user's consent [1].

A common instance is location-based services found in ubiquitous computing. It was suggested that most of these services would usually share information of the requester with the service provider [7]. However, research [2] have showed that people were more comfortable sharing their location and time under their own preference but if the privacy settings on the application they use is more complex, they would not customise those settings and resulted in more sharing of information despite valuing their own privacy of personal information. With various services including social media and video sharing services promoting and requesting of information, it was suggested that privacy is more preserved in a distributed architecture, in which all nodes in a system shares information to other entities such as cloud-based services, in comparison with a centralised approach that would rely on advanced encryption [7]. This is mainly due to an edge intelligence principle such that entities within a system can control the depth of data produced and have their own access control points. Also, entities within a system can choose to provide data only when needed by external entities for specific services [7] such as getting only the name, profile picture and email of someone's Facebook profile as a way of signing up for Spotify. Nonetheless, these profiles are linked with each other and can be used to identify from one application to another. Even with attempts [7] to develop a framework that could preserve privacy without involving a messenger between a requester and service provider, there were limitations on its solution in terms of the information domain and hierarchy in different data used in ubiquitous computing systems. As such, anonymity may be compromised once a party has gotten hold of data from one application as they can then connect to the other linked applications and expanding all of it to user profiling and tracking within the system itself [1,7].

Furthermore, privacy faces challenges in legal issues and self-regulation of users. With different countries having different laws in terms of privacy on the internet, there isn't a standard guideline. For example, Australia's legislation requires all data to be stored and cannot be deleted even if a user has deactivated their account whereas other countries like United States can request their information to be deleted from a database if they wish to. Without proper frameworks around privacy policies around the world, there are difficulties in protecting the data as wireless networks are being accessed globally and being connected globally. For example, a problem would arise if users in America are using a

service provided by Australia but due to American laws, there is a conflict between the user's local laws and the service provider's local laws. This leads to self-regulatory frameworks emerging with a concept of "soft law" to express private commitments that encircles acceptable and expected ethics [11]. Although self-regulation costs less and is more flexible compared to state laws, self-regulation only regulate people who are motivated or principled as not everyone would adopt those rules [11]. For example, in certain pervasive games like Pokemon GO, even though there were bans put around cheaters, many users would still find other ways in spoofing their locations to benefit within the game. While users are not being honest in the information provided, private sectors are also not adhering to standards in providing actual information about how information is collected and tracking profiles of users. As such, national regulations and self-regulations relies on the society and private sectors to be disciplined but this is not accomplishable in many cases.

Development processes

It is important to remember that privacy is not just about third parties getting information, but it also considers permission on using it. Many applications guarantee their information being protected from other third parties but do not consider getting consent about using the information collected and proceeded using them for user tracking and user profiling. In this case, further computation in systems can be done in context-aware applications to measure a user's preference of privacy [4]. Although countries in the European Union have implemented a framework aimed at user control of their data [4], this has not been applied globally and not applicable in context-aware applications. Another possible solution suggested by [11] is for international legislators to complement with private sectors to carry out detailed regulations such that they can contribute in monitoring the process to ensure guarantee of privacy in the Internet of Things. In addition, transparent policies should be in place for what information is being exchanged between users and service providers [1] and designers should make use of design principles to simplify complex privacy settings for users to customize privacy preferences.

User awareness

Users should choose appropriately what information to share with applications and consider if they would feel comfortable revealing those information to the public. They should not rely on anonymity to protect their information and always monitor their own digital footprints. It is also important to be on track of legal acts about data sharing to know their rights but also be reminded that these laws may change as time passes or in case of political changes. Users should also be aware of changes to privacy preferences on applications or devices they use. Keeping personal details online private and not save them on any public devices is also a good way for preventing privacy breaches.

Security

The security of applications covers many aspects in a system including the confidentiality, integrity, availability, and authenticity of keeping data in a system. The main issue surrounding these properties for keeping information safe is the need for the system to be evolutionary. It must be customizable, flexible, and adaptable to extreme environments due to the use of different devices working on varying networks [1,3]. Even with traditional computing, attacks on systems are unavoidable such as the security breach of over 2.5 million PlayStation and Xbox accounts [4]. As such, the security infrastructure of a pervasive computing environment should keep evolving on pace with technology advancement. It also needs to extend beyond the virtual world and implement changes to the real world like preventing unauthorized access to physical smart spaces [3]. The challenge in doing so is running tests to suffice the system. Tests often take time, longer than the rapid technology development in the industry. Therefore, it would be difficult for an "old" system to be still sustainable after it has been released to be able to withstand security breaches from "new" technologies used to attack the system.

Moreover, in pervasive computing, mobility is emphasised in which access points may be outside of a physical space. As such, user authentication is crucial in making sure that the users are authorized to have privileges of accessing the system without being in a space with embedded computing. The verification of contextual information is necessary to eliminate false context information incoming from unidentified or faulty sensors [7]. However,

Development processes

In ubiquitous computing environments, the mechanisms for security needs to be strong in authentication yet non-intrusive. A system can have multiple authentication methods to boost security like the two factor authentication methods applied in some applications now. [3] suggested that biometrics such as fingerprints or retinal scans would be hard to forge and would be preferred over authentication devices. Applications can also use notifications to alert users if the context information differs from their usual information such as having their account logged in from a different location or device compared to their usual context.

User awareness

Users can change their passwords regularly to prevent unauthorized access to their accounts. In whatever situation, users must be vigilant and be aware towards third parties requesting for passwords that will never be asked for by administrations [4]. They can use a password manager to keep their passwords safe and have unique passwords for each interface they use within a pervasive system. Basically, they should never disclose their passwords and take note of any suspicious activities on their accounts.

Trust

As [9] has framed trust, it is a concept that is strongly related to identity management in privacy as well as access control in security. With regards to identity management, it is difficult to assess the accuracy of personal information. As devices are now mobile, the system needs to allow access even without information of a device used by the user. As some personal information may not be true based on user input, it is hard to differentiate between whether a true user is accessing control or another individual pretending to be the user.

Another challenge in trust issues is the evaluation of social relationships to support collaboration. Although there are arguments that trust can increase security that would allow flexibility in design and more access control [1], trust can also be used as an evaluation to maximize the performance of an application through a trust relationship between users and devices [9]. The challenge in ubiquitous systems is that due to the distributed components in the architecture, distributed system architectures are needed such as having a standardized security policy between the components in the system [1].

Development processes

Designers of a system can limit the boundaries of access points such as deploying a framework using low-bandwidth networks based on the environment of which a system is used. For example, Centaurus limits a user to access smart spaces in an office environment from a mobile device connected via Bluetooth [1]. This allows authorized personnel to use the services of another authorized user for collaboration with the condition of an existing trusted social relationship between two users. In addition, the system designed should keep customers' information confidential

User awareness

If users do not trust an application, the easiest way is to not use it. Users should take actions to revoke access to other applications if one of them are compromised in a pervasive system. Users should also be aware of the terms and conditions in using a service or device to decide whether to trust the system or application. In the case of already breached applications, users can try to recover their accounts from the manufacturing company as well as changing the methods of authentication in other applications.

Discussion

Basically, privacy is guaranteed within the properties of security. If a system is secure in protecting personal information from unwanted parties and transparent in its collection and usage of information, a trust relationship between the user and system can be accomplished. Nonetheless, it is still a cycle of having security in exchange of privacy if the system requests for identity information besides context information for secure user authentication and the question of providing the information lies in the trust of the user towards the system. And the trust is dependent on how much privacy and security the system can provide.

Despite existing technologies to take into accounts of the existing challenges faced around privacy, security, and trust, it is important to remember that technology is static in a way that it only acts upon how they are designed to be. Even with machine learning properties, a ubiquitous computing environment is still limited to its algorithmic formulations and comes down to just binary codes. For these systems to be ideal, society must be disciplined. Even with legislations placed around technologies, there will always be vulnerabilities so legal authorities should work with sociologists and psychologists more closely to find a way in reducing threats globally.

Conclusion

This paper provided a general overview of difficulties that pervasive computing face in managing privacy, security, and trust. Especially with the huge collection of amount collected, anonymity cannot be guaranteed especially with state legislations that do not conform to a globalised framework. In terms of security, pervasive computing needs to overcome the obstacle of user authentication in the same pace as technological advancement. Trust is a more complex concept that needs to address the challenges in both privacy and security as well as balancing the two entities to ensure that user satisfaction is guaranteed. Generally, future designers of ubiquitous systems may also need to be well-informed of information security to develop better systems. The key for a trusted system is transparency and strong security covering the users' privacy. For users to be aware, they should take basic actions around prevention, detection, and response towards breaching of information. As these entities encircles a wide area, future works may require more specific research into each of these entities and come up with technical solutions for the challenges faced by ubiquitous computing.

References

[1] Al-Karkhi, A., Al-Yasiri, A., Linge, N. 2012. Privacy, Trust and Identity in Pervasive Computing: A review of Technical Challenges and Future Research Directions. *International Journal of Distributed and Parallel Systems*, 3(3), pp.197-218.

[2] Benisch, M., Kelley, P.G., Sadeh, N., Cranor, L.F. 2011. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, 15(7), pp.679-694.

[3] Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., Mickunas, M.D. 2003. Towards Security and Privacy for Pervasive Computing. In: OkadaM., Pierce, B.C., Scedrov, A., Tokuda H., and Yonezawa A. (eds) *Software Security – Theories and Systems*. Lecture Notes in Computer Science, vol. 2609. Springer, Berlin, Heidelberg.

[4] McGoogan, C. 2017. *Hackers steal 2.5 million PlayStation and Xbox players' details in major breach* [Online]. Available from: http://www.telegraph.co.uk/technology/2017/02/01/hackers-steal-25-million-playstation-xbox-players-details-major/ [Accessed 5 December 2017].

[5] Rahman, F., Hoque, M.E., Ahamed, S.I., Ul Alam, M.A. 2013. Preserving User Privacy in Pervasive Environments with a Collaborative Model. *2013 Seventh International Conference on Software Security and Reliability Companion*, 18-20 June 2013 Gaithersburg. IEEE, 57, pp.2266-2279.

[6] Robinson P., Vogt H., Wagealla W. 2005. Some Research Challenges in Pervasive Computing. In: Robinson P., Vogt H., Wagealla W. (eds) Privacy, Security and Trust within the Context of Pervasive Computing. *The International Series in Engineering and Computer Science*, vol 780. Springer, Boston, MA.

[7] Roman, R., Zhou, J., Lopez, J. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Netowrks*, 57, pp.2266-2279.

[8] Scutti, S. 2017. *The psychology of privacy in the era of the Internet of Things* [Online]. Available from: http://edition.cnn.com/2017/03/22/health/psychology-privacy-wikileaks-internet-of-things/index.html [Accessed 1 December 2017].

[9] Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. 2014. Security, privacy and trust in Internet of Things: The Road Ahead. *Computer Networks*, 76, pp.146-163.

[10] Vigo, J. 2017. *From Snooper's Charter to Sleepwet: A Crisis in Internet Privacy* [Online]. Available from: http://www.huffingtonpost.co.uk/entry/from-snoopers-charter-to-sleepwet-a-crisis-in-internet-privacy_uk_5a1478a3e4b0815d3ce65a90 [Accessed 5 December 2017].

[11] Weber, R.H. 2010. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), pp.23-30.