Anita Chidera Duanne Eluwa
5th April 2021
Cybersecurity Risk Management

Privacy Risk Models for Designing Privacy – Sensitive Ubiquitous Computing Systems

Hong et al. [1] claims that "Privacy" has always been a contentious issue for ubiquitous computing. They also explain that the convergence and increasing widespread deployment of sensors, wireless networking, and devices of all form factors are providing tremendous opportunities for interaction design, allowing us to create systems that can improve safety, efficiency, and convenience. This paper however proposes a privacy risk model as a method to help designers identify, understand, and prioritize privacy risks for applications. They also outlined two different parts of this model. The first part is a privacy risk analysis which poses a series of questions to help designers think about the social and organizational context in which an application will be used, the technology used to implement that application, and control and feedback mechanisms that end-users will use. The second part looks at privacy risk management, and is a cost-benefit analysis intended to help designers prioritize privacy risks and develop architectures, interaction techniques, and strategies for managing those risks. [2]. Before describing the privacy risk model, they placed the risk models in context of some related works. A commonly cited resource in the privacy canon is the set of fair information practices. These guidelines help large organizations, such as corporations and governments, manage people's personal information in a responsible manner. [3] In other words, the goal of the risk model is centered on focusing on the privacy of the individuals rather than on the security of the systems. [4]

In the privacy risk analysis, the first part of the model which includes the set of questions designed to help the designers with the privacy issues was categorized into the Social and organizational context and technology used for the application. The social and organizational context identifies some questions such as who are the users of the system? and the impact of the system to the stakeholders while the technology part discusses how the user's personal information is collected and how long the data is retained. The second part of the model looks at privacy risk management, which takes the unordered list of privacy risks from the privacy risk analysis, prioritizes them, and helps design teams identify solutions for helping end-users manage those issues (through technical solutions, social processes, or other means).[5] In this part, a few questions are discussed. Such as: How does the unwanted disclosure take place? What are the default settings? and a lot more. These sections of the analysis are carefully reviewed before a solution can be proffered. This paper also describes two case

studies using the privacy risk model outlined above. The first case study is the Location-enhanced Instant Messenger, and the second case study is. A BEARS Emergency Response Service. These two studies used lo-fi prototypes and interviews to help with the design. One way of managing these risks is to provide better mechanisms to ensure that only authorized emergency responders see location information. [6] In conclusion, no security threat model is perfect, and just as no task analysis is perfect, no privacy risk model is perfect. No analysis can predict every potential use of personal information. [7] However, a privacy risk model only assists to provide a reasonable level of privacy.

References

[1] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques.*, pp. 91-100, 2004.

[2] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems.," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pp. 91-100, 2004.

[3] A. Westin, "Privacy and Freedom," New York, Athenum, 1967, pp. 16, 487.

[4] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems.," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques.*, pp. 91-100, 2004.

[5] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems.," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques.*, pp. 91-100, 2004.

[6] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems.," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques.*, pp. 91-100, 2004.

[7] J. Hong, J. Ng, S. Lederer and J. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems.," *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques.*, pp. 91-100, 2004.