Perceived Security Risks in Mobile Interaction

Larry Koved, Shari Trewin,
Cal Swart, Kapil Singh,
Pau-Chen Cheng
and Suresh Chari
T.J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
koved@us.ibm.com

ABSTRACT

The broad scale move to mobile devices as a primary computing platform raises a number of issues about how people perceive the security risks when using and relying on these devices for performing sensitive computing tasks. We are studying mobile authentication and authorization, focusing our attention on applications with high security requirements, such as mobile banking, in the context of mobile platforms such as smartphones and tablets. We report on our initial findings with respect to three distinct user groups.

1. INTRODUCTION

Willingness to perform actions for security purposes is strongly determined by the costs to the individual and perceived benefit [1]. When end-users' perceptions of risk are not aligned with those on which the system is based, there is a mismatch in perceived benefit, leading to poor user acceptance of the technology [2]. However, non-experts think and respond to risk very differently than experts [3]. Experts use statistical reasoning to assess risk, whereas non-experts rely on affect [4], and are unduly influenced by the perceived degree of damage that will be caused.

With the rapid adoption of mobile devices as a primary interface to networked services, there are increased risks with respect to authentication and authorization:

- The risk that the user's actions will be observed. If these are authentication actions, this may allow an observer to authenticate on a different device as the user (impersonation).
- The risk that the device is lost or stolen, potentially exposing sensitive information.
- The risk of the possibility of a man in the middle attack, allowing an attacker to capture authentication credentials and perform actions as if he/she were the user.
- The risk of cached passwords on mobile devices. It is difficult to enter (strong) passwords into mobile devices. Also, people have many different passwords to remember. Entry of a password or PIN can consume a large fraction of the time a user is interacting with the device [5]. As a result, passwords and PINs are being cached on the device to improve usability.

To guard against these risks, trustworthy authentication and secure communication are essential. We argue that strong authentication methods based on different authentication methods are one part of a solution. Secure id/password schemes are not sufficient, because passwords are easily observed, and they do not provide assurance that the user is who he/she claims to be. In particular, mobile device applications, including the web browsers, are caching authentication credentials, enabling an attacker to exploit them. Modern smartphones can enable multi-factor authentication by using sensors such as cameras and microphones to capture biometric data. This may be part of a possible solution, but may impose additional burdens on users [6]. This is in direct contrast to users' expectations of fast, efficient interactions on mobile devices. Typical interaction with a mobile device is very brief [5]. Lengthy and complex authentication challenges are a distraction from the user's task. If users do not understand the reason for these authentication demands, they may reject or attempt to circumvent these authentication methods.

Little is known about peoples' awareness of these mobile device authentication risks. We conducted studies to understand end-user perception of risk in mobile transactions and how this can be used to influence acceptance of multi-factor authentication. Key components of our research [7] include:

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

- Conducting studies on the end user perception of risk and using the results to drive mechanisms to align end-user perception of risk with the value at-risk in transactions.
- Use sensors available on mobile phones for multi-factor authentication, including the use of biometric authentication techniques. Part of our approach is to understand the requirements for user-acceptance and lowered friction in authentication.
- Use a risk scoring component to drive the balance between end-user acceptance, value-at-risk and the performance of various authentication techniques.

2. USER STUDY

Our initial study looked at three distinct user groups to understand the security risks they perceive when using mobile devices: technology company workers, people performing "work" via Amazon Mechanical Turk, and IT security experts. Specific scenarios were presented, including the use of an app and the web to do personal banking, accessing confidential company information, accessing medical information, and using a credit card with an unknown online retailer. The risk factors that people identified for these scenarios were organized around ways an attacker could obtain the data or account access credentials. The four primary categories of risk emerging from the study are: shoulder surfing, network attacks, compromise of the device, and untrustworthy remote service providers. All of the identified risk factors relate to the loss of personal or confidential information, including passwords. Larger consequences of loss, including access to personal or company accounts, financial loss, identity theft, and publication of private information, were also identified by the study participants. Another category identified by respondents is risk associated with using a mobile device in a particular situation, e.g. personal safety. Future alternative scenarios may expose further perceived risks.

Our next challenge is to compare these findings with actual risk as perceived by organizations, and identify areas of mismatch between the users' perceptions and the organization. Where there is a mismatch, risk communication with the user will be considered as a means to align user and system perceptions of risk. When user and system perceptions are aligned, there is greater likelihood that users will accept and comply with organizational security requirements such as multi-factor authentication methods.

3. RELATED WORK

Garg and Camp [8] studied peoples' perception of online risks such as viruses, phishing and identity theft, several of which are relevant to mobile contexts as well. Their models of factors that influenced risk perception identified familiarity of the risk and degree of dread associated with that risk as the most significant determinants of perceived risk. Risks that could be easily related to known risks in the physical world were better understood and considered more serious.

Chin, Felt, Sekar and Wagner [9] surveyed smartphone users about their willingness to perform potentially sensitive activities on their phone and their laptop. Participants had some misconceptions about security. For example, some participants concerned about WiFi phone connections did not have similar worries about the same connections when used with a laptop. Furthermore, some participants were suspicious of cellular connections because no password was needed. When asked an open question about their primary concerns about their phone, 28% cited the possibility of losing it, or it being stolen, and the information lost was an important factor in this concern.

Felt, Egelman and Wagner [10] examined the concerns of smartphone users with respect to apps that take actions on their device. In a large survey, they presented possible actions an app might take. Actions that involved financial loss or permanent data loss were of most concern, while actions that were reversible were of least concern. People over the age of 50 ranked risks more highly than those under 30, and women ranked risks slightly higher than men did.

4. ACKNOWLEDGMENTS

This work is supported by a grant from the Department of Homeland Security under contract FA8750-12-C-0265.

5. REFERENCES

[1] Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link' a human /computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122-131, 2001.

[2] Adam Beautement, M. Angela Sasse, and Mike Wonham. The compliance budget: Managing security behaviour in organisations. In *NPSW'08*, September 2008.

[3] Daniel Kahneman, Paul Slovic, and Amos Tversky. Judgment under uncertainty: Heuristics and biases. Cambridge University Press, 1982.

[4] Serge Egelman, Lorrie Faith Cranor, and Jason I. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the 2008 Conference on Human Factors in Computing Systems, CHI 2008*, 2008, Florence, Italy, April 5-10, 2008, pages 1065-1074. ACM, 2008.

[5] Patti Bao, Jeffrey Pierce, Steven Whittaker and Shumin Zhai. Smart phone use by non-mobile business users. *MobileHCI'11. Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, pp 445-454, 2011.

[6] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, Shay Ben-David. Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption. *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC)*, pp. 159--168, 2012

[7] Larry Koved. Usable Multi-Factor Authentication and Risk-Based Authorization. *Cyber Security Division 2012 Principal Investogators' Meeting.* October 11, 2012. http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-3.16-TTA03-IBM-Research-Koved.pdf

[8] Vaibhav Garg and Jean Camp. End user perception of online risk under uncertainty. In *Proceedings of HICCS 2012.* IEEE. pp 3278-3287.

[9] Chin, E., Felt, A., Sekar, V., and Wagner, D. (2012) Measuring user confidence in smartphone privacy and security. *Proceedings of SOUPS 2012.* http://dl.acm.org/citation.cfm?id=2335358.

[10] Felt, A., Egelman, S., and Wagner, D. (2012) I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns. *Proceedings of Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2012),* ACM Press.