Exploiting Human Factors in User Authentication

by

Payas Gupta

Submitted to School of Information Systems in partial fulfillment of the requirements for the Degree of Doctor of Philosophy in Information Systems

Dissertation Committee:

Debin GAO (Supervisor/Chair)
Assistant Professor of Information Systems
Singapore Management University

Xuhua DING (Co-Supervisor)
Associate Professor of Information Systems
Singapore Management University

Robert DENG Huijie
Professor of Information Systems
Singapore Management University

Zhenkai LIANG
Assistant Professor of Computer Science
National University of Singapore

Singapore Management University

2013

Exploiting Human Factors in User Authentication

Payas Gupta

Abstract

Our overarching issue in security is the human factor – and dealing with it is perhaps one of the biggest challenges we face today. Human factor is often described as the weakest part of a security system and users are often described as the weakest link in the security chain. In this thesis, we focus on two problems which are caused by human factors in user authentication and propose respective solutions. a) Secrecy information inference attack – publicly available information can be used to infer some secrecy information about the user. b) Coercion attack – where an attacker forces a user to handover his/her secret information such as account details and password.

In the secrecy information inference attack, an attacker can use publicly available data to infer secrecy information about a victim. We should be prudent in choosing any information as secrecy information in user authentication. In this work, we exploit public data extracted from Facebook to infer users' interests. Such interests can also found on their profile pages but such pages are often private. Our experiments conducted on over more than $34,000$ public pages collected from Facebook show that our inference technique can infer interests which are often hidden by users with moderate accuracy. Using the inferred interests, we also demonstrate a secrecy information inference attack to break a preference based backup authentication system Blue Moon™. To mitigate the effect of secrecy information inference attack, we propose a new authentication mechanism based on user's cellphone usage data which is often private. The system generates *memorable* and dynamic fingerprints which can be used to create authentication challenges. In particular, in this work, we explore if the generated behavioral fingerprints are *memorable*

enough to be remembered by end users to be used for authentication credentials. We demonstrate the application of memorable fingerprints by designing an authentication application on top of it. We conducted an extensive user study that involved collecting about one month of continuous usage data from 58 Symbian and Android smartphone users. Results show that the fingerprints generated are remembered by the user to some extent and that they were moderately secure against attacks even by family members and close friends.

The second problem which we focus in this thesis is human vulnerability to coercion attacks. In such attacks, the user is forcefully asked by an attacker to reveal the secret/key to gain access to the system. Most authentication mechanisms today are vulnerable to coercion attacks. We present a novel approach in generating cryptographic keys to fight against coercion attacks. Our technique incorporates a measure of user's emotional status using skin conductance (which changes when the user is under coercion) into the key generation process. A preliminary user study with 39 subjects was conducted which shows that our approach has moderate false acceptance and false rejection rates. Furthermore, to meet the demand of scalability and usability, many real-world authentication systems have adopted the idea of responsibility shifting, where a user's responsibility of authentication is shifted to another entity, usually in case of failure of the primary authentication method. In a responsibility shifting authentication scenario, a human helper who is involved in regaining access, is vulnerable to coercion attacks. In this work, we report our user study on 29 participants which investigates the helper's emotional status when being coerced to assist in an attack. Results show that the coercion causes involuntary skin conductance fluctuation on the helper, which indicates that he/she is nervous and stressed. The results from the two studies show that the skin conductance is a viable approach to fight against coercion attacks in user authentication.

Contents

List of Figures

List of Tables

Publications arising from this thesis

1. Payas Gupta, Swapna Gotipatti, Jing Jiang, and Debin Gao. Your love is public now: Questioning the use of personal information in authentication. In *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '13, New York, NY, USA, 2013. ACM (**Chapter 3**)

2. Payas Gupta, Tan Kiat Wee, Narayan Ramasubbu, David Lo, Debin Gao, and Rajesh Krishna Balan. Human: Creating memorable fingerprints of mobile users. In *Tenth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom*. IEEE, 2012 (**part of Chapter 4**)

3. Payas Gupta, Kiat Wee Tan, Narayan Ramasubbu, David Lo, Debin Gao, and Rajesh Krishna Balan. Design and implementation of human memorable fingerprints. Technical Report SMU-SIS-13-100, Singapore Management University, Mar 2013 (**part of Chapter 4**)

4. Payas Gupta and Debin Gao. Fighting coercion attacks in key generation using skin conductance. In *Proceedings of the 19th USENIX conference on Security*, USENIX Security'10, Berkeley, CA, USA, 2010. USENIX Association (**Chapter 5**)

5. Payas Gupta, Xuhua Ding, and Debin Gao. Coercion resistance in authentication responsibility shifting. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '12, New York, NY, USA, 2012. ACM (**Chapter 6**)

Acknowledgements

To the casual observer, a doctoral dissertation may appear to be solitary work. However, to complete a project of this magnitude requires a network of support, and I am indebted to many people.

This thesis would not have been possible without the support of many people. Many thanks to my adviser, Debin Gao. I am very grateful for the opportunity to work with him and could not have imagined having a better mentor for my Ph.D study. Working with him has definitely sharpened my research ability and helped me grow as an individual and a professional. Perhaps the most important lesson I learned from him was how to effectively convey my thoughts and ideas in both written and spoken mediums. I admire his ability to balance research interests and personal pursuits.

Furthermore, I am very grateful to my committee members, Robert Deng, Xuhua Ding, and Zhenkai Liang, for their guidance, support, insightful comments and hard questions.

In addition, I would like to express my deepest appreciation to Steve Miller, Dean of School of Information Systems, Singapore Management University, whose enthusiasm for "quality research" and "big ideas" have significantly improved my work and inspired many new research directions.

Besides my advisor and committee members, I am very privileged to work with Rajesh Krishna Balan, Narayan Ramasubbu and David Lo. Their technical excellence and tremendous grasp of experimental issues had a great impact on me. Without them I could not have excelled in conducting user studies effectively.

I would like to express my sincere thanks to Living Analytics Research Center at Singapore Management University for giving me the opportunity to spend a year in Carnegie Mellon University as a research scholar. Furthermore, I am very grateful to Adrian Perrig, for his insightful comments in my studies, for many motivating discussions and guidance throughout my stay at CMU. The work done in collaboration with him has helped me to explore other areas.

Very special thanks to Ong Chew Hong. She helped me in all my user studies, answering to all sorts of questions and going out of her way to help me out in recruiting participants. None of the work in this thesis and my other research projects could have been possible without her support. She is a gem of a person. Above all, she made me feel a friend, which I appreciate from my heart. Besides her I would also like to thank Seow Pei Huan for her help.

During my stay at Singapore Management University and at Carnegie Mellon University, I have made many friends and they have been vital in making the Ph.D. process a fun and enriching experience. I want to thank Pawan Gupta, Varun Khanna, Salman Hamid, Aditya Maru, Vivek Desai, Roger Cherian, Yash Divadkar, Ankit Birla, Prem Prasoon, Darshan Santani, Husain Kagalwala, Manu Nahar, Sudhanshu Nahata, Meryl Gotlieb and Nancy Beatty for taking an extra mile to help me out in day to day life. In addition, I have been very privileged to get to know and to collaborate with many other great people who became friends over the last several years. I appreciate Swapna Gottipati, Yan Qiang, Kartik Muralidharan, Sougata Sen, Jun Han, Han Jin, Noi Sian and Tey Chee Meng for their friendship, collaboration and encouragement.

I would like to specially thank Varunika Goyal for her love and encouragement. And, thank you for your support when I have needed it the most. Thank you with all my heart!

Above all, I am thankful to my parents and my sister Kopal Gupta for their support and love who endured this long process with me.

To my loving parents, Kusum Gupta and Vijendra Gupta.

Chapter 1

Introduction

An integral part of computer security is user authentication, which seeks to confirm the identity of a user for the purpose of granting individual users access to their respective accounts. All security access methods are based on four fundamental pieces of information: something the user is, something the user has, something the user knows, and recently proposed someone the user knows [23]. If the user of the system can provide proof in some or all of these areas, he/she is admitted to the system. To protect the user and the communication between the user and the system, there are many security software solutions available. However, even using the very best software, which implements the most advanced technology and the most secure algorithms, cannot guarantee 100% security because the end users are humans and humans are gullible in understanding security concepts.

The human factor is the underlying reason why many attacks on computers and systems are successful. The human factor is often described as the weakest part of a security system and users are often described as the weakest link in the security chain. It has been noticed that attackers always try to exploit the weakest link. For example, researchers have shown how attackers can exploit human activity on public forums and online social networking websites to mine personal attributes (e.g. age, sex, sexual orientation) and sensitive information (e.g. answers to challenge questions such as mother's maiden name). Another human naiveness in understand-

ing security concepts is in dealing with passwords for different accounts. Having so many accounts, humans can no longer remember all the passwords resulting in duplication of passwords. Sometimes they either use simpler passwords which are not good enough to reliably defend against dictionary attacks or use stronger passwords which are too complicated to be remembered and write them down on a piece of paper. Though not the focus of the thesis, but to demonstrate a few more human factor exploitation in user authentication; attackers do not target on-line banking directly. Instead, they attack the bank's customers, using phishing techniques to trick them into giving away their credentials. Although widespread deployment of the Secure Sockets Layer (SSL) helps protect password authentication against passive eavesdropping attacks, it does little to help users resist more devious threats, such as phishing. Alternatively, an attacker can call the IT help desk, pretend to be a senior manager and gain access to confidential information. This is social engineering - exploiting human vulnerabilities rather than technical ones.

From this dissertation we would like to highlight that any information or an entity which can be used to exploit the vulnerability of a system is a valuable resource to the attacker. This information can be used to harm the user; being it side channel information, inferred information or the user himself/herself. Specifically, in this dissertation we formulate and propose solutions to two authentication problems relating to human factors. a) Secrecy information inference attack – where publicly available information can be used to infer secrecy information about the user. b) Coercion attack – where an attacker forces a user to handover his/her secret information such as account details and password.

Using personal and private information in generating challenges for authentication systems has been there for a long time e.g. in backup authentication (mother's maiden name) when the user forgets the login details of the primary account. In a backup authentication, a user's responsibility of authentication is shifted to another entity, usually in case of failure of the primary authentication method. In recent years, online social networking activity has increased a lot and because of the avail-

able platforms like Facebook more and more people are sharing private information online. People show their support to a number of things in public e.g. by clicking on the Facebook 'like' button. In this work, we first show how an attacker can exploit the public data extracted from Facebook to infer users' undisclosed interests on their personal profiles. We also show how this inferred information can be used to break a preference based backup authentication system and demonstrate why we should not use weak personal information e.g. "interests" in the generation of challenges. To resist the secret information inference attack, we design a system called HuMan (History based User Centric Memorable ApplicatioN). HuMan generates memorable and dynamic fingerprints from the user's cellphone usage data which can be remembered by the user and can be posed as a challenge during authentication.

However, all security mechanisms fails when the user is succumb to coercion attacks i.e. putting a gun on the user's head and coercing him/her e.g. to enter his/her bank account details. The user has no choice but to comply and reveal his/her secret. This is an extreme form of human factor exploitation. For that we propose to build a coercion resistant system. For a system to be coercion attack resistant, it is required that when the user is under coercion, he/she will have no way of generating the secret, or the secret generated will never be the same as the one generated when he/she is not being coerced. If this requirement is met, then an adversary would not apply any threat to him/her because the adversary understands that the user would not be able to generate the secret when he is threatened to do so. We demonstrate this attack under two scenarios (when the user is forced to reveal his own secret and when the user is forced to reveal someone else's secret) by conducting two separate user studies and hence propose to use emotional response (skin conductance in our case) as a parameter to fight against such attacks.

In the following sections, we individually highlight the attacks and demonstrate through various user studies which evince how different resources can be obtained to exploit human factors in user authentication. We also demonstrate the human factors which should not be used in creating authentication challenges.

1.1 Fighting against secrecy information inference attack in user authentication

In a secrecy information inference attack, user's secret information can be leaked from the publicly available data. Prior research shows that the information shared on the web with a limited set of users can still leak undisclosed privacy attributes, e.g., users' interests and even sexual orientation [149, 115]. Authors of [29] crawled Facebook users' personal profiles (which are often private) to infer users' undisclosed interests. Private data can only be obtained by either crawling user's personal profile on social networking sites or taking explicit permission from the user. However, getting access to the private data is not as easy as compared to the public data. Facebook, for example, has made all the fan pages public by default [44]. Access to the data of these pages can be conveniently obtained through Graph APIs [45]. Mining private information from public data is not easy mainly due to the large amount of noise contained in the heterogeneous pages, and the huge amount of unstructured data involved. In this work, we first demonstrate that this belief might not be true in certain aspect. In particular, we show how we can obtain data from Facebook and use it to infer users' interests that can usually be obtained only from their personal and often private profile pages. This information can be used in many ways including targeted spamming, showing ads without the consent of users, or even breaking into specific authentication systems. To demonstrate the security and privacy implication of this, we base our experiments on mining personal interests to break into Blue Moon^{TM} [81] introduced by RavenWhite as a backup authentication system to provide better security and usability. Our experiments conducted on over more than 34K public pages collected from Facebook and data from volunteers show that our inference technique can infer interests that are often hidden by users on their personal profile with moderate accuracy. We are able to disclose 22 interests of a user and find more than 80,097 users with at least 2 interests. From our findings, it is clear that we should be prudent in choosing the information to create

authentication challenges because attackers can use the publicly available interests data from Facebook to break into authentication systems like Blue Moon™.

Considering this, we propose to use an authentication system based on personal data which is resistant to secrecy information inference attack. The authentication challenges are generated dynamically and the user can still remember without requiring any extra effort. We built a system, called HuMan, which generates fingerprints from user's cellphone usage data. We explore if the generated behavioral fingerprints are memorable enough to be remembered by end users. The dynamicity and memorability of these fingerprints can also eradicate human factors like human memory interference, sharing of secrets etc. We evaluated the memorable fingerprints generated from this rich multi-context data by asking each user to answer various authentication questions generated from the fingerprints. We conducted an extensive user study that involved collecting about one month of continuous usage data from 58 Symbian and Android smartphone users. Results show that the fingerprints generated by HuMan are remembered by the user to some extent and that they were moderately secure against attacks even by the people who knows a lot of information about the user i.e. intimates and acquaintances.

1.2 Fighting against coercion attack in user authentication

Many techniques have been proposed for secure communication and authentication. Some of these techniques, e.g., those using biometrics [58, 116, 119, 120, 53], offer desirable security properties including ease of use, unforgettability, unforgeability (to some extent), high entropy and etc. However, most of these schemes are not resistant to coercion attacks in which the adversary uses physical force, e.g., wielding a gun, to coerce the trustee to comply [130]. When the user's life is threatened by an attacker, one would have to surrender the secret, and the system will be com-

promised despite all the security properties described above. This is an extreme form of exploitation of human factor in user authentication to gain access to the system. Specifically, we present a novel approach to protection against rubber hose cryptanalysis i.e. coercion attacks in generating cryptographic keys. For a cryptographic key generation technique to be coercion attack resistant, it is required that when the user is under coercion, he/she will have no way of generating the key, or the key generated will never be the same as the one generated when he/she is not being coerced. If this requirement is met, then an adversary would not apply any threat to him/her because the adversary understands that the user would not be able to generate the key when he is threatened to do so. We explore the incorporation of user's emotional status (through the measure of skin conductance) into the process of key generation to achieve coercion resistance. With 39 participants in our user study, we find that our technique enjoys moderate false acceptance rate of 3.2% and false rejection rate of 2.2% in key generation.

Furthermore, to meet the demand of scalability and usability, many real-world authentication systems have adopted the idea of responsibility shifting, explicitly or implicitly, where a user's responsibility of authentication is shifted to another entity, usually in case of failure of the primary authentication method. One example of explicit responsibility shifting is in the fourth-factor authentication whereby a user gets the crucial authentication assistance from a helper who takes over the responsibility [23]. Facebook also uses a similar authentication protocol which allows the user to recover his account's password by collecting vouch codes from his trusted friends [46]. There is also implicit responsibility shifting which might not seem as obvious. For instance, whenever suspicious activity is detected in a user account, the system administrator takes over the responsibility of revoking the attempted authentication. In the fourth-factor authentication system [23], subverting the helper allows the adversary to log in without capturing the password of the user. When the trustee to whom the responsibility has shifted is another computer system, we can use any standard security mechanism to protect it. However, when such a trustee

is a human being, protection becomes non-trivial because of the potential coercion attacks. We remark that it is unclear whether the same technique could help in protecting the trustee in our study. The difference between the trustee and a victim in general coercion attacks is subtle, yet critical in terms of security. No prior study has shown the effect on emotional status of trustee in this case and his skin conductance. Therefore, the crux of our work is to investigate whether the trustee's skin conductance also changes under coercion, and if any, whether the magnitude of change is large enough to be captured by the coercion resistance technique. We design and conduct a user study involving 29 university students to evaluate the trustee's emotional status in a simulated coercion attack. The results of our user study are positive with false acceptance rate of 3.1% and false rejection rate of 1.7%. This shows that the victim's skin conductance still changes under physical threats. The principles of our findings in this study are applicable to other authentication mechanisms as well.

The rest of this dissertation is organized as follows: Chapter 2 reviews the existing studies on authentication and human factors which can be exploited to gain illegitimate access to the system. In Chapter 3, we demonstrate a secrecy information inference attack on a preference based authentication system using the public data extracted from Facebook. In Chapter 4, we argue how we can use the private data from the user's cellphone to create authentication challenges which are memorable and resistant to secrecy information inference attack. We then present an extreme case of human factor exploitation i.e. coercion attack in Chapter 5 and propose a solution to fight against this attack in generating cryptographic key. In Chapter 6, we extend our work to verify if the solution presented in the previous chapter can be used to fight against coercion attack in authentication responsibility shifting. Finally, we conclude with future direction of the current research in Chapter 7.

Chapter 2

Literature review

Authentication has been studied by cryptographers, security engineers, human-computer interface designers, linguists, ethnographers, and others. This chapter will survey the diverse academic literature with particular focus on the security research motivating this dissertation. As every authentication mechanism requires some involvement of humans and humans are considered to be the weakest link in the security chain, therefore, in this chapter we discuss some of the prior works done in the area of human factors in authentication. Related work specifically to this dissertation has been described in individual chapters.

Memory interference and limits Passwords are by far the most used and most easily subverted method of personal authentication. The use of secret words to authenticate humans has ancient origins. It also appears in folklore, famously in the tale of Ali Baba and the forty thieves (first translated into English in 1785 [148]), with the protagonist using the phrase "open sesame" to unseal a magical cave. Ominously, Ali Baba's greedy older brother Qasim forgets this password during the course of the story with disastrous consequences.

If an organization institutes policies to ensure secure passwords (such as frequently changed alphanumeric upper/lower case combination of at least 10 characters) the inconvenience is so great that such a policy will be violated in an overwhelming number of cases. The use of alphanumeric usernames and passwords

is the most often used (and also the cheapest) method of computer authentication [102]. However, unfortunately human beings are limited in their information processing capabilities [33, 114]. People either use simple passwords that are easy to remember but easy to crack or use difficult passwords which are difficult to remember. According to [168], there are very few people who do not deviate from the best practices for password use. Users either use the same password all the time, or use relatively simple passwords; re-use their old password; write passwords down either on paper or store it in an electronic file without protecting it; share passwords with others, etc.

Many recommendation and techniques including using pictures instead of passwords [38, 35, 89], passface [25], pass-phrase [143] etc have been suggested in the past by taking into consideration of user's knowledge [2, 138, 173]. These schemes suffer from the same problem of memory interference; scalability is a major issue. For schemes like passphrases, usability studies of passphrases [97] have found them to be just as memorable as passwords, subject to an increased rate of typographical errors. Users may find it difficult to remember so many different pass-phrases for different accounts. Moreover, systems need to manage a database of a huge number of images, so that they can prevent guessing and DDOS attacks.

Sharing of secrets The argument — "if you don't have anything to hide you won't mind sharing passwords" is the chief weapon in the arsenal of the password sharers. We are always told not to share our passwords or bank account PINs with others, but the rule is harder to apply when it's your significant other who wants to check those party pictures in your Facebook account [37]. In a recent study [107], authors found that roughly one in three online teens (30%) reports sharing one of their passwords with a friend, boyfriend, or girlfriend. While passwords may be guarded closely by some youth, password sharing among peers can be a sign of trust and intimacy. Online girls are much more likely than online boys to share passwords with friends and significant others (38% vs. 23%), and older teens ages 14-17 are more likely to