5-2012

Coercion Resistance in Authentication Responsibility Shifting

Payas GUPTA
Singapore Management University, payas.gupta.2008@smu.edu.sg

Xuhua DING
Singapore Management University, xhding@smu.edu.sg

Debin GAO
Singapore Management University, dbgao@smu.edu.sg

DOI: https://doi.org/10.1145/2414456.2414512

Coercion Resistance in Authentication Responsibility Shifting

Payas Gupta
School of Information Systems
Singapore Management University
payas.gupta.2008@phdis.smu.edu.sg

Xuhua Ding
School of Information Systems
Singapore Management University
xhding@smu.edu.sg

Debin Gao
School of Information Systems
Singapore Management University
dbgao@smu.edu.sg

ABSTRACT

Responsibility shifting, a popular solution used in the event of failure of primary authentication where a human helper is involved in regaining access, is vulnerable to coercion attacks. In this work, we report our user study 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. This response can be used to strengthen the security of the authentication system by providing coercion resistance.

Keywords

Coercion resistance, biometrics, authentication

General Terms

Human factors, Security

1. INTRODUCTION

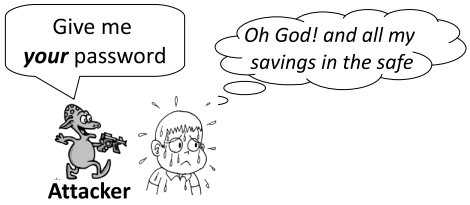
To meet the demand of scalability and usability, many real-world authentication systems have adopted the idea of responsibility shifting, explicitly or implicitly, where a user's responsibility of authentication is shifted to another entity, usually in case of failure of the primary authentication method. One example of explicit responsibility shifting is in the fourth-factor authentication [1] whereby a user gets the crucial authentication assistance from a helper[1] who takes over the responsibility. 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 [2]. There is also implicit responsibility shifting which might not seem as obvious. For instance, whenever suspicious activity is detected in an user account, the system administrator takes over the responsibility of revoking the attempted authentication.

[1]The helper is said to be the fourth factor as someone the user knows.

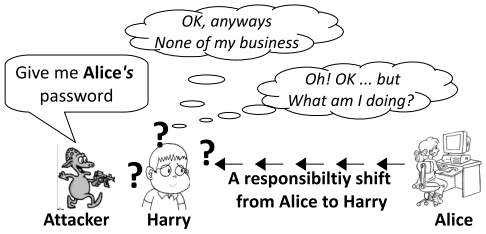
ASIACCS '12, May 2–4, 2012, Seoul, Korea.

Responsibility shifting does *not* enhance the security of the authentication. Instead, it entangles with the authentication scenario and may weaken its security. A system that relies on alternate email addresses for password recovery is only as secure as whoever managing those alternate email accounts. The provider of the alternate email account could become the victim of an attack in an attempt to break the authentication in the primary system. In the fourth-factor authentication system [1], 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*. In a coercion attack, the adversary uses physical force, e.g., wielding a gun, to coerce the trustee to comply. To the best of our knowledge, this is the first work to study the security of human trustees under coercion attacks in a responsibility shifting in authentication.



(a) When forced to reveal his own password



(b) When forced to reveal someone else's password

Figure 1: Coercion attack in different scenarios

The existing techniques against coercion attacks [3] rely on the fact that the victim's skin-conductance (an emotional response parameter [7]) changes involuntarily upon coercion, resulting in incorrect authentication credentials. We remark

that it is unclear whether the same techniques 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, see Figure 1.

The victim shown in Figure 1(a) (and studied in [3]) is coerced to reveal *her own* credential. The consequences include the victim's account being broken into, and her valuable being stolen. It is therefore naturally believed (and experimentally verified) that the victim becomes nervous under such an attack. In contrast, Harry, the trustee considered in this paper (see Figure 1(b)), is coerced to provide *Alice's credential*, direct consequence of which does not inflict any harm on himself. No prior study has shown the effect on emotional status of Harry 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.

To put our study into a concrete example, we focus on the fourth-factor authentication [1], a recent proposal on shifting responsibility to help backup authentication. We first provide an overview of the fourth-factor authentication protocol and discuss in detail the potential coercion attack on it. As the main contribution in this paper, we then 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 in the sense 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.

2. FOURTH-FACTOR AUTHENTICATION AND COERCION ATTACKS

As discussed in Section 1, fourth-factor authentication [1] is a typical example of responsibility shifting. In this section, we first provide an overview of the protocol used in the fourth-factor authentication, and then discuss a potential coercion attack when responsibility shifting takes place. Finally, we provide background on a recent technique [3] that fights against coercion attacks.

2.1 Fourth-factor authentication protocol

In fourth-factor authentication, a trustee (Harry) to an account holder (Alice) is another registered user of the system who can authenticate himself successfully and is usually a person who knows Alice, e.g., a work colleague. He can verify Alice's identity via any social means, e.g., by recognizing Alice's face or voice over the phone, when the responsibility to authenticate Alice is shifted to him. Here we provide an overview of the fourth-factor authentication system which consists of the authentication server (AS), Alice (U) who needs help in her authentication, and Harry (H) to whom the responsibility to authenticate is shifted.

Enrollment: U provides AS with a list of members $\mathsf{L_U}$ to whom a responsibility to authenticate can be shifted in case of emergency authentication.

Responsibility shifting: In case U loses her hardware token tk (but has password p), she shifts the responsibility to H to authenticate herself. U first initiates the authentication process by contacting AS and sending p to partially authenticate with AS. U chooses a helper H from $\mathsf{L_U}$, and asks for help to verify her identity to AS. H verifies the identity of U (by recognizing her face or voice), and then authenticates himself to AS and obtains a vouch code vc for U. H subsequently passes vc to U using the same means (over the phone or face-to-face). Finally, U sends vc to AS, and AS verifies vc and authenticates U.

This completes the fourth-factor authentication.

2.2 Potential coercion attacks

Note that the responsibility shifting extends the trust base to authenticate Alice from one person (the owner of the account, i.e., Alice) to two persons (Alice and Harry). In Section 2.1, Harry together with "half of Alice" (who only has p and loses her hardware token) manage to authenticate Alice to the system. The attacker who has stolen the other half of Alice (the hardware token) could potentially use the same protocol to impersonate Alice if he gets the help from Harry (e.g., by coercing Harry). This responsibility shifting enables the attacker to extend his coercion target from Alice (who could be an important person heavily armed) to any registered helper (who could be much easier to coerce). Therefore, from Alice's perspective, assigning a helper could potentially make her account less secure. From Harry's perspective, by agreeing to be the helper of Alice, he might run into the risk of attracting coercion attacks on himself due to the new capability he has on Alice's account.

We reiterate that such a coercion attack exists in any responsibility shifting to authenticate in general, e.g., Facebook trust based authentication [2], although in this paper we use fourth-factor authentication as a concrete example for better explanation.

2.3 Coercion resistance

Gupta et al. proposed a technique to fight against coercion attacks using skin conductance in cryptographic key generation [3]. Here, we provide a brief overview of it since it is used to process data captured in our user study.

During enrollment, features from the skin conductance samples are extracted and modeled to feature descriptors, the mean and standard deviation of which over a finite set of training samples are calculated in order to tolerate small deviation of a user's skin conductance. A two column lookup table is created where each entry of the lookup table either contains a valid key share or some garbage value. Valid key shares are extracted from the lookup table during authentication to reconstruct the key.

The idea is that if a feature descriptor bit is reliable, i.e., its mean μ and standard deviation σ always satisfy $t_{\mathsf{SC}} \in [\mu - k*\sigma, \mu + k*\sigma]$ where k and t_{SC} are parameters to acquire a trade-off between the usability and security, then a valid key share in placed in one of the columns and the other column contains some garbage bits. If a feature descriptor bit is unreliable, then both columns contain valid shares (typically different). This ensures that "correct" descriptors (when users are not coerced) lead to valid (non-unique) keys. To be able to authenticate all the valid keys, a unique string $\mathcal{B}$ is generated for each user, which is then encrypted with all possible valid keys that can be derived from the lookup table. Upon the end of the enrollment, the service provider stores a template containing the lookup table and all the encrypted values and $\mathcal{B}$.

During authentication, a feature descriptor is generated from the user's fresh SC sample. This feature descriptor is

compared with t_{SC} to generate a bit string called the feature key. This feature key is then used to find corresponding shares from the lookup table to recreate a cryptographic key. The generated key is used to decrypt all the stored values and if the decrypted value of $\mathcal{B}$ matches with $\mathcal{B}$, then the user is authenticated to the service provider.

3. USER STUDY

In a coercion attack, the adversary uses physical force, e.g., wielding a gun, to force the victim to comply. When the victim's life is threatened, she would have no choice but to follow what she is ordered to do. Therefore, a critical element to fight against coercion attacks is victim's involuntariness, i.e., defenses must *disable* the victim to perform what the adversary orders her to do.

The first and only comprehensive proposal was due to Gupta et al. [3] in using skin conductance to generate cryptographic keys (see Section 2.3). However, as discussed in Section 1, the scenario their technique applies to is substantially different from responsibility shifting discussed in this paper, where the coercion victim (Harry) is forced to reveal *someone else's* credential (vc for Alice) instead of his own. This raises an important question as whether the requirement of victim's involuntariness still holds here, i.e., whether Harry will be nervous or stressed (which leads to involuntary change of his skin conductance and a different cryptographic key) under such a coercion.

We answer this question by designing and conducting a user study. Obviously, we cannot "really" coerce the participants in our study, but have to mimic a scenario that is close enough while passing our Institutional Review Board (IRB)'s evaluation. In this section, we first discuss the difficulties and complexity involved in designing this user study. We then explain the participant demographics and the experimental procedure. Results of the user study are shown in Section 4.

3.1 Difficulties and complexity

The challenge of this user study is to mimic the context of responsibility shifting. For Harry to take over the responsibility from Alice in an authentication, he needs to know her well so that he is able to verify her identity by recognizing her face or her voice. Therefore, one approach of the user study would be to ask two participants (probably friends) to come together. However, this poses a concern as we need to coerce Harry to reveal some personal/privacy information of Alice. Such coercion might lead to a negative impact on the participants' friendship, and is therefore not desirable (would not pass IRB evaluation).

We propose another strategy whereby one participant plays the role of Harry with two conductors (researchers) playing the role of Alice and the adversary ($\mathcal{M}$) respectively. Such a setting eliminates the concern of breaking the friendship of the participants, but would need to satisfy the following criteria.

1. Harry (the participant) should hold some secret of Alice (a researcher) which $\mathcal{M}$ (another researcher) doesn't know (or Harry believes that $\mathcal{M}$ doesn't know).

2. Harry should know this secret before $\mathcal{M}$ tries to coerce him to reveal the secret.

3. Harry should believe that if this secret is leaked to $\mathcal{M}$, then there will be some severe consequences on Alice or on Alice's personal/private data.

Moreover, another difficulty to overcome is to find the right balance between the research requirement of applying sufficient pressure on the participant so as to mimic a coercion attack, and the human rights requirement of no physical or mental harm to the participants.

3.2 Participants and initial setup

Considering the stress on the participants, we decided to concentrate on the younger generation (undergraduate and graduate students in the age from 18 to 30). We have altogether 30 participants, from which one participant was not able to understand the story presented during the user study. Therefore, we have only successfully performed our experiments on 29 participants, out of which 14 were male and 15 were female. Participants were compensated with $20 (equivalent currency) for their participation in the study.

Since many previous works have shown that skin conductance is a reliable and convenient way of measuring one's emotional status [3], we used a skin conductance device (similar to the one used in [3]) to monitor the skin conductance response SC of the participant. Initially, there was an incomplete disclosure regarding the purpose and the steps of the study in order to ensure that the participants' responses are not affected by the knowledge of the research.

The user study was carried out in a relatively small room with two laptop computers for Alice and Harry to use. Although Harry was informed that both are Alice's personal and work computers (see Phase-I in Section 3.3), we denote these two computers as Alice's computer and Harry's computer in the rest of this paper for the sake of clarity. Alice's computer was used to capture the skin conductance of Harry, and Harry's computer was the vehicle for the responsibility shifting as well as coercion attacks (see the detailed procedures below). We developed a small program running on Alice's smartphone which can lock Harry's computer remotely. Alice carried the smartphone in her pocket and used it to lock Harry's computer without being noticed by Harry.

3.3 Experimental Procedure

The user study is divided in four phases.

3.3.1 Phase I. Passing the secret to Harry

Aim — This is to satisfy criteria 1 and 2 discussed in Section 3.1. A secret of Alice is passed to Harry while making Harry believe that $\mathcal{M}$ knows nothing about the secret.

Procedure — At the start of the experiment, Harry is greeted by Alice in the room. Alice informs Harry that both computers are hers (personal and work use), and nicely asks Harry not to delete or modify any existing data. After Harry settles down in front of one computer, Alice remotely locks it with her smartphone, and tells him to use password "keepMeSecret" to unlock it. This password becomes the secret Harry knows about Alice and $\mathcal{M}$ will later coerce him to reveal it.

Note that the secret in our study is passed from Alice to Harry directly. This is different from the real world responsibility shifting where the secret is usually passed from an authentication server or another entity. We remark that this would not have changed the results of the user study, as long as the third criterion stated in Section 3.1 is satisfied.

3.3.2 Phase II. Gathering normal skin conductance data

Aim — We need to capture the skin conductance response level when Harry is calm to set a baseline (normal emotional state) before coercing him.

Procedure — We play a video by showing pleasant (geographical) pictures with soothing music when capturing Harry's skin conductance.

3.3.3 Phase III. Portraying $\mathcal{M}$ as a bad guy

Aim — Since we cannot really coerce Harry with, e.g., a gun pointing to his head, we mimic the coercion in a way that is acceptable to the IRB. The simulated coercion has two steps. First, we make Harry believe that $\mathcal{M}$ is a bad guy, and secondly, $\mathcal{M}$ will "coerce" Harry to do something inappropriate (i.e., revealing Alice's secret in Phase IV of the user study).

To make the attack scenario appear real for Harry, we also make an impression in front of Harry that $\mathcal{M}$ is aware of the fact that Harry knows Alice's secret (the password that unlocks Harry's computer in Phase I). This mimics the context of coercion attack in responsibility shifting that $\mathcal{M}$ knows that Harry has taken over the responsibility of Alice's account.

Procedure

1. $\mathcal{M}$ walks into the room and asks Alice (in a slightly rude manner) to leave the room. Alice then walks out.

2. $\mathcal{M}$ walks to Harry's laptop, opens the password manager of the web browser and starts writing down the passwords on a piece of paper. $\mathcal{M}$ makes sure that Harry observes what he is doing on the laptop.

3. In a short while, Alice returns and $\mathcal{M}$ acts like he is in the situation of embarrassment (idiom: "caught with pants down"). $\mathcal{M}$ immediately closes the password manager.

4. Alice presses the button on her smartphone to lock Harry's laptop (without being noticed by Harry), and then asks Harry to enter the password to unlock it (without speaking out the password). All these take place when $\mathcal{M}$ is in the room.

5. $\mathcal{M}$ behaves rudely while talking to Alice and subsequently leaves the room.

6. Alice explains to Harry that $\mathcal{M}$ is her classmate, and inquires what $\mathcal{M}$ has done during her absence. No matter whether Harry mentions the details or not, Alice badmouths $\mathcal{M}$, which further convinces Harry that $\mathcal{M}$ is really a bad guy.

3.3.4 Phase IV. Coercing Harry

Aim — This is to capture Harry's skin conductance response when $\mathcal{M}$ coerces him to reveal Alice's secret.

Procedure

1. $\mathcal{M}$ enters the room again and rudely demands that Alice leave the room.

2. This time, Alice walks to Harry's computer and manually locks the screen before leaving the room.

3. After Alice leaves, $\mathcal{M}$ walks over to Harry's computer and starts guessing the password. After a few trials, $\mathcal{M}$ verbally "coerces" Harry to reveal or enter the password. Sentences used by $\mathcal{M}$ include "I will complain to my professor and he will take strict actions against you", "Don't act smart, I know that you know the password".

Toward the end of the user study, we explain to the participants the real motivation of the study and provide a questionnaire to find out their experience during the whole study. Note that Harry's skin conductance is continuously measured throughout the study.

4. EVALUATION

We present the results of the user study and our interpretation of the results in this section. As discussed in Section 1, there is a subtle yet important difference between the coercion received by someone in a non-responsibility-shifting scenario [3] and Harry in our user study. The difference is whether the victim is coerced to reveal her own secret (or the secret that protects her own valuables) or someone else's secret. Therefore, we first analyze what participants felt when they were being coerced to reveal Harry's laptop's password. Building upon that, we then state our hypotheses and based on approach proposed previously [3] we analyze how many participants were actually nervous and stressed. Here, we assume that Harry might be using such a system to protect Alice's secret he has, and evaluate the false-alarm rate and miss rate of the system. After that, we analyze the participants' responses to the questionnaire to have a better understanding of the collected skin conductance data. The participants' responses to the questionnaire are noted on a 1–5 Likert scale: strongly agree (●), somewhat agree (◐), neutral (⊖), somewhat disagree (◑) and strongly disagree (○). Finally we discuss the design and some of the limitations of our user study.

4.1 Did Harry feel nervous and stressed?

We first review the participants' questionnaire responses to check whether they *felt* nervous and stressed during the coercion. According to the results obtained for our 29 participants, 86% of the participants felt nervous and stressed, and the rest feeling neutral. This has two important implications. First, our user study design is largely a success, in the sense that we have achieved the goal of mimicking coercion on the participants. Second, it seems that most people do feel nervous and stressed even when coerced to reveal someone else's secret, which is the main question our user study seeks to answer. Four out of the 29 participants did reveal the password of Harry's computer, whose comments include the following when inquired.

- "I was intimidated and gave in the password";
- "I was not comfortable when the bad guy was forcing me to enter the password";
- "It was not my password and data";
- "Alice can always change her passwords later on".

Comments from those who did not reveal the password include "it is not ethical to give away someone else's secret information to other", "it is not a good idea to get involved in

someone else's personal conflicts", "I was not sure of the kind of personal data residing in the researcher's (Alice) laptop".

4.2 Was Harry really nervous and stressed?

Skin conductance has been shown in many previous studies to be a reliable indication of one's emotional status [8]. If participants actually feel nervous in a responsibility-shifting scenario, we envision that one could build a coercion-resistant system using skin conductance. To better understand the extent to which such a system could be successful, we evaluate its accuracy in detecting coercions.

We first state our two hypotheses that

- **Hypothesis 1:** The trustee whom the authentication responsibility shifts to becomes nervous and stressed upon a coercion attack;
- **Hypothesis 2:** What the participants have experienced in the user study presented in Section 3 and what the trustee would experience in a coercion attack in the fourth-factor authentication follow the same distribution.

We simulate the execution of the system built upon a previous proposed coercion-resistant system [3] (see section 2.3) and evaluate our two hypotheses stated with the skin conductance data captured during our user study. We then evaluate its accuracy in terms of false-alarm rates (a correct cryptographic key generated when Harry is coerced) and miss rate (an incorrect key generated when Harry is calm). We define a user as calm/nervous if the key generated during authentication does/does not match against the key generated during enrollment.

The system is trained with 10 out of 26 SC samples (randomly chosen with a duration of 10 seconds) captured during Phase II (when Harry is calm, see Section 3.3), and is tested with the remaining 16 SC samples in Phase II (to calculate the miss rate) as well as all SC samples in Phase IV (to calculate the false-alarm rate). Figure 2 shows the results with three different settings of k (k is used to tolerate some errors in the skin conductance response) and several different settings of t_{SC} (t_{SC} is a threshold value); see Section 2.3 for details.

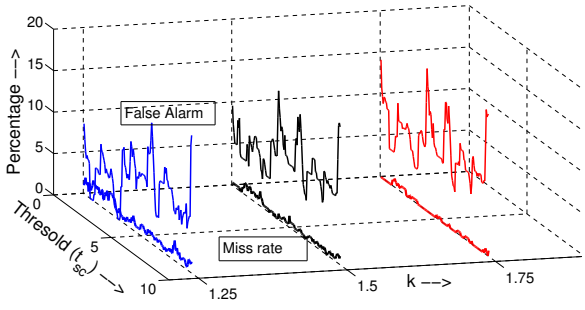


Figure 2: False-alarm and Miss rate

We observe relatively low false-alarm and miss rates of our system built under our hypotheses. For example, when $k = 1.25$ and $t_{SC} = 3.1$, we obtained a false-alarm rate of 3.1% and a miss rate of 1.7%, which are comparable to those originally obtained in a non-responsibility-shifting scenario [3] (false-alarm rate of 3.2% to 3.1% and miss rate of 2.2% to 1.7%). This, in general, shows that Harry was nervous and stressed when coerced to reveal Alice's secret, and the combination of our two hypotheses are good explanations to the data observed during the user study. We also found from the skin conductance of those 4 participants who revealed the password of Alice's laptop during coercion were all nervous and stressed.

A closer look at Figure 2 shows that the false-alarm rates are higher than the miss rates. One possible explanation to this is that some participants were not nervous for the whole period of Phase IV of the user study. The "coercion" applied to Harry in our user study is not as severe as a real-world coercion attack, which leads to inaccuracy in our hypothesis 2 and an increase to the false-alarm rate.

4.3 Personal v/s someone else's secret

In this subsection, we focus specifically on Hypothesis 1 to see how the difference between being coerced to reveal one's personal secret and being coerced to reveal someone else's secret could have affected its validity. Note that this is also part of the main question we aim to answer.

We have presented to every participant the following two statements and asked for their responses. Results are shown in Table 1.

S-1. In the real world, you feel *nervous* when being coerced to reveal *someone else's* secret information (e.g., email account password).

S-2. In the real world, you feel *nervous* when being coerced to reveal your *own* secret information (e.g. email account password).

		Revealing someone else's secret				
		●	◐	⊖	◑	○
Revealing your own secret	●	6	12	2	0	0
	◐	1	4	0	1	0
	⊖	0	1	1	0	0
	◑	0	0	0	1	0
	○	0	0	0	0	0

Table 1: Nervous when being coerced to reveal secret information?

From Table 1, we notice that the number of participants above the diagonal (highlighted) are higher (those feeling more nervous when revealing their own secret) as compared to that below the diagonal (those who feel more nervous when revealing someone else's secret). The result seems to follow common sense, although this does not necessarily preclude the possibility of designing a coercion-resistant system for either case since the change of skin conductance may still be large enough to be captured. To get an idea of this point, we perform some simple analysis on the skin conductance captured in this study and that captured in another one [3]. We found that in our user study the change in the SC data is actually higher (μ=5.18, σ=2.58) as compared to (μ=1.86, σ=1.28).

We warn readers from drawing more than what it deserves from such a simple analysis. First, the two studies are quite different, and a direct comparison of the skin conductance captured does not have a strong basis. Second, although

changes in skin conductance have been shown to be a reliable indicator of emotional status [8], it has not been shown that the value of skin conductance reflects the extent to which the user feels nervous. That said, we believe that our simple analysis could be viewed as an evidence that skin conductance does change when they are coerced to perform involuntarily, regardless the ownership of the secret.

4.4 Limitations of our user study

There are two main limitations of our user study. First, Alice is played by a female member of our research team in our user study. Since people in general show compassion towards female gender, our results could be biased. Secondly, as the user study is an act, many unforeseen events did take place. The actual scenarios were not always consistent throughout the user study across different participants.

5. RELATED WORK

In this section we review some of the techniques which involve implicit/explicit responsibility shifting and some previous work on emotion recognition. To the best of our knowledge, this paper is the first work on stress detection under the context of responsibility shifting. As explained in Section 1, an explicit responsibility shift occurs when a user fails to reproduce her credential where an implicit shift occurs in case when there is some suspicious activity in the account etc. In both cases the entity to which the responsibility is shifted can be either "human" or a "computer system".

There have been many proposals on explicit shifting of responsibility when the user fails to generate her credentials. Alternate email addresses can be used to reset the password of the primary email-id in the case of password loss [10]. Other backup authentication mechanism includes personal knowledge based questions [6, 5], preference based backup authentication mechanism [4], and the fourth factor authentication [1]. Facebook has added a security feature similar to fourth-factor authentication where a user can recover his account by collecting the codes from 3 of his trusted friends [2]. Authentication schemes involving responsibility shifting are always vulnerable to coercion attacks as long as the trustee is a human being.

Recently Twitter (using implicit responsibility shifting) automatically revoked access to those third party apps abusing its APIs for users tweet collection [9]. This is also an example of implicit responsibility shifting whereby the responsibility is shifted to a computer system checking whether the number of API calls are exceeding the limit or not.

Skin conductance is an emotional response parameter and is associated with a wide variety of feelings, thoughts and behavior. Researchers have linked skin conductance response to stress and autonomic nervous system arousal [8]. There are many techniques proposed for emotion recognition, among which Gupta et al. [3] proposed the first and comprehensive approach to use skin conductance as an emotion recognition parameter to fight against coercion attack, though it is not for responsibility shifting.

6. CONCLUSION AND FUTURE WORK

In this work, we study the security of human-trustee based authentication responsibility shifting, in particular, under coercion attacks. Our intensive user study shows that most trustees demonstrate nervousness when being forced to reveal others' secret, which can be captured by their involuntary skin conductance changes. We envision that this change could be used to develop coercion-resistant systems for responsibility shifting in authentication.

7. ACKNOWLEDGMENTS

The authors wish to thank Swetha Sharmista Nittala for her assistance in conducting the user study.

8. REFERENCES

[1] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security*, CCS '06, pages 168–178, New York, NY, USA, 2006. ACM.

[2] Facebook. What are trusted friends? security. `http://www.facebook.com/help/?faq=119897751441086`.

[3] P. Gupta and D. Gao. Fighting coercion attacks in key generation using skin conductance. In *Proceedings of the 19th USENIX conference on Security*, USENIX Security'10, pages 30–30, Berkeley, CA, USA, 2010. USENIX Association.

[4] M. Jakobsson, L. Yang, and S. Wetzel. Quantifying the security of preference-based authentication. In *Proceedings of the 4th ACM workshop on Digital identity management*, DIM '08, pages 61–70, New York, NY, USA, 2008. ACM.

[5] M. Just. Designing and evaluating challenge-question systems. *Security & Privacy Magazine, IEEE*, 2(5):32–39, 2004.

[6] M. Just. On the design of challenge question systems. *IEEE Security and Privacy*, 2:32–39, September 2004.

[7] K. H. Kim1, S. W. Bang, and S. R. Kim. Emotion recognition system using short-term monitoring of physiological signals. *Medical and Biological Engineering and Computing*, 42(3):419–427, May 2004.

[8] H. Selye. *The Stress of Life*, chapter 1-7. McGraw-Hill, 1956.

[9] A. Tsotsis. Twitter revokes automatic 3rd party dm access, gives users more details on app permissions. TechCrunch. `http://goo.gl/SJDQf/`.

[10] M. Wu, S. Garfinkel, and R. Miller. Secure web authentication with mobile phones. In *DIMACS Workshop on Usable Privacy and Security Software*, 2004.