In the Balance in Saudi Arabia: Security, Privacy and Trust

Abstract
Bank policies must meet their clients requirements to provide effective security. However, bank policies in the Kingdom of Saudi Arabia seem to run contrary to their clients requirements when they prevent them from sharing their authentications with their family. We investigated Saudi participants behaviour towards authentication and found that credentials are shared between couples as a sign of mutual trust. This, may extend to siblings and parents too. The consequence of such behaviour is that these account holders are liable for any loss, and this also increases the opportunities for so-called spouse attacks. Saudi bank policies need, at one and the same time, to match their clients behaviour and simultaneously to provide complete and effective security for them.

Author Keywords
Authentication; Security; Privacy; Trust

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous.

General Terms
Human factor, Authentication
Introduction
The main goal of policies adopted by banks is to protect the bank and its users. Such policies have been designed to enable secure business processes for both bank and clients. Those policies must be usable otherwise they would be unable to provide effective security. However, when the bank policy makers designed their policies, they focused mainly on providing secure rules to protect the bank and failed to give enough consideration to the requirements and activities of their clients. In order to create effective, utility-based systems, a realistic notion of user behaviour must be included. People will not follow rules made by security experts and developers if these rules go against their normal behaviour, or against their culture and values [15].

This study focuses on Saudi behaviour towards the authentication information required for them to access their bank accounts (credit card and online banking). Bank systems in the Kingdom of Saudi Arabia normally require a card plus a personal identification number or PIN to authenticate their users when they use an automated teller machine (ATMs), or a combination of user number, password and one-time PIN for online banking use. The main issue we have uncovered pertains to policies about online banking, with Saudi banks requiring their clients to not share their account authentication information with others. If a bank user in Saudi Arabia decides to share their bank account password with others, the consequence is that they are then liable for any losses incurred from misuse. According to the Electronic Banking Rules for the Saudi Arabian Monetary Agency (SAMA) (clause 3-3 Bank Obligations) “Banks are responsible for providing secure and safe systems and services for their customers unless the customer fails to safeguard their account user number or password and divulges it to a third party”[9]. This is not the case for credit and debit cards, where a client can choose to authorize another to use their card. SAMAs Regulations for the Issuance and Operation of Credit and Charge Cards (clause 7-1) state: “The client (i.e. the cardholder) is not liable for any non-authorized transactions made with his card after it has been reported lost or stolen if the following conditions have been satisfied.” and the third condition is: “The client must exercise every care and vigilance in safeguarding his card from loss or theft or unauthorized use.” The document defines unauthorized use as “The use of a credit card or debit card by anyone other than the client (card holder) who does not have actual or implied authorization”[10]. This behaviour can also cause additional problems in the case of partners becoming estranged, e.g. when separating or divorcing. In those situations, there is higher risk of so-called spouse attacks; attacks that are usually extremely successful because the attacker has privileged knowledge of their victim (and spouse) – for example, knowledge of their authentication details. Our main area of interest is to investigate the factors that might affect the decision to share this information with a family member, and also to explore how well the consequences of that behaviour are understood. If routine behaviour towards bank account passwords were understood, guidelines could be established to support security roles that are consistent with Saudi behaviour, culture, and standard practices. In addition this could underpin regulatory policy and allow security principles to be designed that are compatible with local, social and cultural practice.

Related Work
In a study investigating how people manage their money and banking on the one hand, and their relationships on
the other, it was found that it was usually one person in a couple who managed the money issues (for example: paying bills, checking the account online, etc), and that it was the same person who checked both the joint and the individual accounts (i.e.; the accounts of the partner). The authors concluded, "Security design should take into account social and cultural practice and enable the sharing of passwords" [14]. Two further studies were carried out in Australia, where the authors argue that it is trust that underpins the sharing of a bank account password between Australian couples rather than lack of awareness that this information is confidential. If couples did not share such information, it was a sign of lack of trust [12, 13]. Meanwhile, in a study carried out in India, it was found that controlling a joint bank account was done by husbands. Wives often do not have any information about the money in that account and neither deposit nor withdraw money from that account [11]. In a study of Arab couples in long-distance relationships, Alsheikh et al. noted that: "Five out of six of our females reported that their partners knew the passwords to all of their online profiles, email and instant messaging accounts, whereas this was the case for only one out of the five males" [1]. In [7] the researcher also discusses sharing passwords with close friends or colleagues, as well as family members. While these studies provide very useful information, we were additionally interested in exploring the implications of spouse attacks on the sharing of credentials.

Case Study Research Approach
The methodology in this study is grounded theory [6, 5, 3]. This serves the goal of this study in that it permits the researcher to understand users behaviours towards the authentication of their bank accounts. Grounded theory makes it possible to understand the reasons behind these behaviours. This is achieved by understanding the behaviour of a small number of bank clients in depth and in detail rather than providing a statistical record of activities of a large number of clients. Grounded theory requires simultaneous involvement in collecting data collection, coding and analyzing data and using comparative methods in order to provide an analytic account of the qualitative data [3]. Eventually, a theory emerges that is based on empirical data. To collect the data, semi-structured interviews have been used [2]. The advantage of this approach arises from allowing the participants to speak in depth about specific issues, without their views being forced to conform with whatever the researcher wishes to hear, and reveal the reasons behind an action or behaviour.

Data Analysis
The interviews were carried out and transcripts made in Arabic because this was the participants language of choice. Creating interview transcripts allows the researcher to notice repeated words and phrases and provides help to recover data that the researcher might have missed during the interview [8, 4]. To generate a theme from the transcript, open coding has been used to identify parts of the data that were similar in meaning. Thereafter, substantive and theoretical coding was undertaken so as to compare these themes from the material emerging from the transcripts as a whole. This process was then repeated until no more themes were found or generated

Participants
Six participants were subsequently interviewed:

- All the participants were Saudi citizens: 3 males and 3 females, all aged 27 years and above.
• All were married. Some of the participants were married for two years and some for over ten.

• Two of the participants were married to each other but they were interviewed separately.

• The participants were from different cities across Saudi Arabia.

• All were employed except one, who was the partner of an employee.

• Three of the participants had a monthly income of between SR 5,000 – SR 10,000; two SR 10,000 – SR 20,000; one less than SR 5,000.

The interviews were conducted on the telephone and lasted 35 – 50 minutes. Conducting the interviews via telephone was acceptable to all participants because the culture is conservative and religious. Since the researcher is a female stranger, it was preferable (especially for male participants) to conduct the interview by using telephone than face-to-face. In addition, in Saudi Arabia commonly there are separate places for females and males for example in schools, universities, government departments, banks so it was easier to conduct the interview via telephone than conduct it in the work or public places. As a cultural norm, it is not usual to conduct interviews with strangers in houses even if both the participant and researcher are from the same gender.

New Ground Covered by the Research
This research will enrich the data on the culture in Saudi Arabia relative to sharing bank authentication information within family members. In addition, it is hoped that it will increase the information available on spouse attacks, specifically in Saudi Arabia, where there is a dearth of studies. The current banking rules in Saudi Arabia do not allow passwords to be shared. As a result of these findings, it is hoped that new guidelines will emerge for the design of security and for policy regulation for the eleven different bank authorities in the Kingdom.

Preliminary Results
• Sharing card authentication (PINs) between couples is a sign of trust between the two parties. This trust is a consequence of marriage and it arises during the first months of the relationship. This is what happened in all six cases.

• Four participants declared that withholding such information between couples is sign of distrust. In the study, only one case admitted to distrust and that occurred while temporarily divorced\(^1\). After the couple had decided to come back together, the participant could not trust her husband again so she decided not to share such sensitive information. He, however, still shares his credentials with her.

• The relationship between couples is stronger than the relationship between siblings.
  – None of the participants shared their online banking credentials with their siblings, but two shared their credit card PINs.
  – If the money in their accounts reached a certain level, participants stated that they would cease to share their PIN with their siblings but would continue to share them with their partner.

\(^{1}\)In Islam, couples may obtain a temporary divorce for three months. If they are able to fix their problems during this period, they are permitted to come back to each other and continue their life normally. If not, this temporary divorce becomes permanent. This process can be used only twice during the life of a marriage.
– Sisters shared their PIN with their brother(s) until they got married, after which such sharing stops.

• The participants gave the following reasons for sharing their authentication with either their partner, their siblings or their parents:
  – Mutual trust.
  – The money in their accounts did not amount to much.
  – To make their life easy and comfortable.
  – Having children increased the likelihood of sharing between couples although they may have started before having children.
  – All the participants relied on receiving an SMS on their personal mobile phone if a transaction were carried out on any of their accounts.

• Female participants declared that they shared their credentials because they suffer from limited freedom of movement\(^2\). However, if that limitation did not exist they stated they would still share, but not as much as they do now.

• Five participants declared that they rarely shared their online bank password with their partners, but the reason was because they used their credit card more than online banking.

• The partner with more IT experience in a couple was responsible for the online banking for both (in one case the woman was responsible, and in another it was the man). When both had equal IT experience then each was responsible for his/her online banking, a situation unaffected by sharing the same device to access the online accounts.

• Knowledge of bank policies was both limited and very general among all participants

• All the participants’ children in this study were under 9 years, thus we did not investigate behaviour involving children.

• All the participants declared that neither their partner nor their siblings or parents would carry out a spouse attack in the case of death or divorce. What gave them the confidence was that:
  – Their partner, sibling(s) and parents were religious people.
  – They considered such behaviour alien to Saudi culture and rare.

Conclusions
Sharing credentials within Saudi families happens regularly and is a sign of trust between family members. As this behaviour is against Saudi online banking policies, account holders are not legally protected. Bank policy makers need to redesign their policies to reflect their clients’ behaviour and to protect them. This study indicates that banks authority in Saudi Arabia need to participate more in educating their clients about security principles. Future studies will seek to further confirm these results.

References

\(^2\)Women are prohibiting from driving in Saudi Arabia.
Computer supported cooperative work, CSCW '11, ACM (New York, NY, USA, 2011), 75–84.


