Forgotten your responsibilities?

(How password recovery threatens banking security)

Ben Smyth

School of Computer Science,
University of Birmingham, UK
www.bensmyth.com

July 20, 2010
(Initial draft: April 12, 2010)

The online banking systems offered by the Lloyds Banking Group (including Bank of Scotland & Halifax) and the Royal Bank of Scotland Group (including Natwest, Royal Bank of Scotland & Ulster bank) are vulnerable to a remote attack which allows an adversary to commit financial fraud. The vulnerability has arisen as a result of poor software engineering practice which neglected security in favour of usability. More precisely, authentication systems are coupled with credential recovery mechanisms to permit the authentication of customers whom have forgotten their credentials; these secondary authentication mechanisms are insecure due to their reliance on publicly available information. In addition, the attack allows the financial privacy of customers to be compromised. These failures are particularly interesting to the design of online banking systems and legal cases in which customers are found liable for fraud. In these cases banks may refuse refunds and assert negligence, or blame the customer for fraud. The attacks presented in this paper may help explain false accusations of liability and help introduce public policy changes which force banks to be held accountable for systems which they have designed.

1 Introduction

Online banking is prevalent in our society due to the convenience it offers. However, the technology presents security problems for banks; as can be observed by the cost of online banking fraud which totalled £59.7 million during 2009 in the UK, a fourteen percent rise on the previous year [The10]. Traditional authentication mechanisms are therefore deemed insufficient and the banking industry has sought more sophisticated systems.

Phishing and malware (in particular, keyloggers) have been attributed as a key source of fraud [The10]. Accordingly banks have adopted different approaches to collecting authentication data, such as, requiring partial information, rather than complete passwords, and relying on drop-down menus as opposed to textfields. Another approach has been the adoption of the Chip Authentication Program (CAP) for multi-factor authentication. CAP is a protocol for EMV smartcards (that is, the credit and debit cards issued by banks) which combines something you have, namely the smartcard, and something you know, namely the smartcard's Personal Identification Number (PIN), to remotely authenticate bank customers.

Authentication systems are ubiquitously coupled with credential recovery mechanisms to allow the identification of customers whom have forgotten their credentials (hence the common usage of "*forgotten your password?*" to refer to such services). For usability and financial reasons, these services are typically executed by geographically remote participants utilising communication channels such as the Inter-

net or telephone system. A combination of personal questions and email-based identification have been used by credential recovery mechanisms to authenticate customers.

The fundamental notion underlying credential recovery mechanisms is that customers cannot remember arbitrary strings, that is, customers should be assumed to forget authentication credentials. The concept of personal questions must therefore avoid this human limitation. Accordingly, personal questions should completely determine customer responses. Moreover, to maintain the security of the authentication system the set of answers should be secret between banks and customers.

Email-based identification and authentication is dependent upon the hypothesis that a customer can be authenticated by demonstrating the ability to receive email sent to a pre-arranged address. Such systems must assume that the vulnerability of email to man-in-the-middle attacks is negligible. Furthermore, only customers are assumed to have access to email accounts.

Contribution. This paper demonstrates how credential recovery mechanisms for the online banking systems offered by the Lloyds Banking Group (including Bank of Scotland & Halifax) and the Royal Bank of Scotland Group (including Natwest, Royal Bank of Scotland & Ulster bank) can be exploited by an adversary to commit financial fraud. More precisely we demonstrate that the set of answers to personal questions are not secret between banks and customers; and, in the case of the Lloyds Banking Group, that the adversary is able to access the email accounts of customers (without launching a man-in-the middle attack). Furthermore, it is argued that the current practice for credential recovery mechanisms are inherently unsafe. Finally, alternative solutions are presented.

The study of these attacks is particularly interesting because it may help explain the cases in which customers bear the cost of financial transactions, when they are adamant that they did not authorise such payments. In such cases the banks may assert blame on the basis that audit trails suggest customers

authenticated; this paper shows how such claims can be false.

Related work. Zviran & Haga [ZH90] and subsequently Podd, Bunnell & Henderson [PBH96] conducted empirical studies on personal questions. They found that close friends, family members and partners were able to immediately answer over 30% of questions correctly. Similar results were discovered by Schechter, Brush & Egelman [SBE09] who studied the four most popular webmail providers. Bonneau, Just & Matthews [BJM10] studied the security of such questions with respect to statistical guessing. Guidelines for the use of personal questions have been introduced by Just [Jus04] and for email-based authentication by Garfinkel [Gar03]. In the context of online banking Schechter *et al.* [SDOF07] and Mannan & Van Oorschot [MVO07] have studied security and usability. An explicit study of personal questions for banking systems was conducted by Rabkin [Rab08]. Subsequently, Smyth [Smy10] demonstrated how weak banking authentication mechanisms could be exploited to violate personal privacy. In this work we examine how vulnerabilities can be abused for financial gain.

2 Case studies

In this section we examine the credential recovery mechanisms used by the online banking systems provided by the Lloyds Banking Group (Section 2.1) and the Royal Bank of Scotland Group (Section 2.2). These systems are both reliant on personal questions, and in the case of the Lloyds Banking Group email-based identification. The security of these questions are particularly weak (Section 2.3) and we show how the systems can be exploited to commit financial fraud (Section 2.4). In addition, the implications for financial privacy are also discussed (Section 2.5).

2.1 Lloyds Banking Group

An attack can be launched by visiting the websites belonging to the Lloyds Banking Group (including

Bank of Scotland & Halifax) and selecting the *"Forgotten sign in details / access suspended?"* option. This launches a credential recovery mechanism which requires knowledge of two of the following pieces of customer information:

1. Father's first name

2. Mother's first name

3. Place of birth

4. First school

These details are available in the public domain and accordingly should be assumed to be known by an adversary. The answer to a user generated question is also required. The adversary must then gain access to the customer's email account to complete the authentication process.

The adversary is now permitted to completely reset all of the aforementioned security questions and is able to take complete control of the customer's account. We remark that the adversary may also require a customer's username (under the assumption that they do not already have this value), but this can trivially be recovered as part of the credential recovery process using the customer's email address.

2.2 Royal Bank of Scotland Group

Online banking services operated by the Royal Bank of Scotland Group (including Natwest, Royal Bank of Scotland & Ulster bank) can be similarly exploited. An attacker visits the target web page and selects the *"Forgotten any of your log in details?"* option. This launches an alternative authentication mechanism which requires knowledge of the following pieces of customer information:

1. Name

2. Date of birth

3. Sixteen digit card number

4. Three digit card security code

5. Sort code

6. Account number

These details should be considered public knowledge and therefore known by an adversary.

Once an attacker has authenticated to the system, using the alternative authentication mechanism, payments may be made to *previous payees*, that is, accounts to which payments have been previously made. It follows immediately that an attacker is able to impersonate a customer to steal funds. A video demonstrating the attack is available online [SS10].

2.3 Attack feasibility

The feasibility of these attacks are dependent upon the adversary's ability to derive the customer data as previously summarised, and in the case of the Lloyds Banking Group the adversary's ability to access a customer's email account. The availability of customer data and email access are linchpins to these attacks and the feasibility of such assumptions will now be studied. First three types of adversary will be distinguished.

Insiders have personal relationships with the customer, for example, partners, family, friends, lodgers, cleaners and co-workers.

Merchants conduct commercial relationships with the customer. These relationships may be direct, for example, landlords, hoteliers and retailers; or remote, for example, telesales staff and e-tailers.

Outsiders have no relationship with the customer.

The distinction between different classes of adversary allows us to better analyse the attacker's capabilities with respect to obtaining customer data and accessing email accounts.

2.3.1 Availability of customer data

It is immediately apparent that insiders can trivially acquire the necessary customer information [ZH90, PBH96, SBE09, Ops10, McK10]. The focus of this section will therefore be merchants and outsiders.

Merchants. Previous research suggests the required customer information necessary to access services provided by the Lloyds Banking Group can be found online [Rab08], in particular on social networking sites such as Facebook [Ops10, McK10], and discovered in public records [GJ05]. Finally, user generated questions, and associated answers, have been shown to be insecure [JA09]. The authentication mechanism is also susceptible to statistical guessing [BJM10] which would facilitate automated attack. Merchants may also be able to make use of corporate databases to discover further details where necessary.

In the case of the Royal Bank of Scotland Group, it is reasonable to assume merchants can acquire card details, that is, the sixteen digit card number and three digit card security code. A merchant whom has direct physical contact with the customer can learn card information during the course of a financial transaction and a remote merchant will be supplied such information by the customer. Any argument that the customer should not give a merchant their card at any point during a face-to-face transaction (in particular, when using chip-and-pin technology) can be waived due to lack of customer education, or simply by social engineering techniques. The customer's surname and sort code can also be learnt from the card, or will be supplied to the merchant for billing purposes. Acquiring the customer's date of birth is trivial, for example: such information is regularly provided to hoteliers during check-in; disclosed to obtain products such as movies and alcohol (which require 'proof of age'); submitted alongside business expense claims; and even published on the Internet, in particular on social networking sites. It remains to consider how the customer's account number can be derived. Account numbers appear on cheques or may be provided for billing purposes, for example, when setting up a direct debit or standing order. (Note that unlike some UK banks, the cards belonging to customers of the Royal Bank of Scotland Group do not contain the account number.)

Outsiders. The customer details required for the Lloyds Banking Group, can be acquired online and in public records, as previously discussed with respect to merchants. Again we reiterate that the susceptibility to statistical guessing permits automated attack.

The banking services offered by the Royal Bank of Scotland Group require knowledge of a customer's banking details. This information should be assumed to be in the public domain and hence available to outsiders. Organised criminals may access these details through the trading of financial data [FPS07, HEF09, Sym10] and a variety of other techniques may also be employed, for example: dumpster diving; third party data loss (for example, those similar to the HMRC incident in 2007 [Hou08, Poy08]); and malware (in particular, keyloggers). Note that the keylogger approach is of particularly concern since it permits automated attack. In addition, outsiders whom are employed by the Royal Bank of Scotland Group, or are acting in collaboration with bank employees, have access to this data.

2.3.2 Access to email accounts

In addition to the aforementioned data, the Lloyds Banking Group also require access to a pre-arranged email address for credential recovery. The plausibility of this will be shown by demonstrating that attackers can gain access to email accounts, without launching a man-in-the-middle attack (that is, we maintain the assumption that the possibility of a man-in-the-middle attack is negligible). Many webmail accounts support *"Remember Me"* technology, whereby a user remains logged in. Insiders are typically in a position to abuse this feature to access a customer's email. A limited number of merchants may also be able to exploit such a feature, for example, landlords, hoteliers and Internet Cafés. It should also be noted that the possibility of man-in-the-middle attacks become non-negligible to such adversaries when customers do not utilise secure connections to email providers. Finally, the results of Schechter, Brush & Egelman [SBE09] suggest that 10-20% of the four most popular webmail providers are accessible to outsiders. These findings are supported by the recent compromise of accounts belonging to Sarah Palin [BBC08] and Twitter executives [BBC09].

Organised criminals may also purchase email accounts on the black market. Figures produced by

Symantec [Sym10] suggest that accounts were available for \$1-20 in 2009. In addition, it is possible to register email addresses of expired accounts, thereby taking control of online services previously associated with that address; the vulnerability of email-based authentication to this kind of attack is largely dependent upon the time-frame since the email address was pre-arranged between the customer and bank.

2.4 Attacks for profit

The attack presented against the Lloyds Banking Group allows an adversary to take full control of a customer's account and therefore immediately facilitates financial fraud. Attacks for profit against the Royal Bank of Scotland Group are slightly more complex, since additional security mechanisms are in place for money transfers. Once a customer/adversary has authenticated using systems offered by the Royal Bank of Scotland Group it is possible to transfer money to previous payees, that is, accounts to which payments have previously been made. Transferring money to new payees requires authentication using CAP and is therefore more secure[1]. It follows that the adversary must be able to access the account to which funds were transferred to gain financially from an attack. The adversary must therefore be either: a payee of the account holder (for example: insiders including ex-partners, lodgers and cleaners; and various merchants); or acting in collaboration with a payee, possibly employing techniques such as bribery, blackmail or violence to gain the payee's cooperation.

Bank employees. The threat of malicious bank employees, or employees under duress, is of particular concern since they have access to customer data. In the instance of the Royal Bank of Scotland Group it would be possible for bank employees to setup payees to which funds could be transferred without CAP authentication. As a prerequisite bank employees would need sufficient privileges within the banking system to setup a payee; it would then be possible to authenticate as a customer using the aforementioned

---

[1]In this paper we do not consider possible flaws in CAP.

techniques and transfer funds. Furthermore, the audit trail would provide evidence that asserts the customer liable for such a transaction.

2.5 Privacy implication

The privacy issues surrounding improper authentication have previously been discussed [Smy10]. In particular, an adversary is able to view all transactions made by a customer; allowing an insight into an individual's personal life. Steven Murdoch, a security researcher at the University of Cambridge, presents an extreme consequence of such an invasion [Tur10]: *"consider a woman who has left an abusive relationship and is hiding from her violent ex-partner, [...] then disclosing where transactions are being made could be potentially very harmful to her personal safety."*

In the context of the legal system financial privacy encompasses the requirement to protect financial information from unauthorised access. Indeed, in the UK this interpretation is supported by the Data Protection Act 1998 which mandates the use of appropriate technical measures to ensure the security of personal data.

The perspectives of society and the legal system clearly dictate the need for financial privacy. However, this work demonstrates that the Lloyds Banking Group and the Royal Bank of Scotland Group have failed in their duty to protect the financial privacy of their customers.

3 Solutions and further work

It should be apparent from the previous section that the vulnerabilities identified against online banking systems offered by the Lloyds Banking Group and the Royal Bank of Scotland Group pose a real threat to the financial security of customers. In this section the unsuitability of current personal questions will be highlighted and possible solutions identified. Henceforth customers are assumed unable to remember arbitrary strings, otherwise they would be able to remember their credentials [Rab08].

3.1 Sensitive personal questions

Rabkin [Rab08] observed that the security of current personal questions is derived from the hardness of an information-retrieval problem. As we move further towards an online society the hardness of this problem, and therefore the security of personal questions, will diminish. Accordingly, the current use of personal questions is inherently unsafe. However, the concept can be enhanced using *sensitive personal questions*, as will now be discussed.

Banking systems contain a wealth of personal financial data and certain information can be used at a particular moment as a shared secret between banks and customers. For example, recent transaction history may serve such a purpose. Further research is needed to explore whether such information can be used to derive questions which enhance security.

3.2 Alternative channels

In addition to the Internet, a number of other communication channels are available between banks and customers. The suitability of these channels for authentication purposes will now be considered.

In-branch. The most secure mechanism for a bank to authentication a customer is in-branch. Primarily this follows from the bank's ability to examine documentation which supports the acclaimed identity of a customer. In addition, the risk and economic cost of attacking in-branch authentication is typically greater than remote attacks. However, despite the increased security of in-branch authentication, it is becoming an unreasonable burden for customers as society moves towards an era of remote banking. Moreover, banks want to avoid the associated cost.

Automated Teller Machines. Automated Teller Machines (ATMs) authenticate customers with respect to their smartcard and Personal Identification Number (PIN), that is, a shared secret between the customer and bank. In terms of attacks for financial gain, ATM access provides more power to the adversary than access to online banking because ATMs allow cash withdrawals (whereas online banking only permits cash transfers between accounts). Accordingly ATMs could be used for credential recovery. However, efficiency of online banking services would be eroded and moreover ATM software would need to be upgraded.

Post. In the UK, the postal service is assumed to provide a secure channel between banks and customers. It is typically used to distribute cards and their associated PINs. Accordingly, it should be deemed a suitable channel to distribute credentials. However, the channel is inefficient and moreover expensive. In addition, it is unsuited to: purely electronic banking, customers living in shared accommodation and frequent travellers.

Telephone. A customer-to-bank telephone channel suffers the same weaknesses as an online system; and moreover, is subject to social engineering vulnerabilities. Bank-to-customer telephone channels should not be used to assume the identity of the customer due to the frequency at which phones are replaced or lost – an estimated 10,000 phones are left in the back of licensed London taxis every month according to Credant Technologies. Furthermore, phones are frequently shared and are easily accessible to insiders. In addition, telephone communication is expensive. Finally, research [LM09] by Zane Lackey, iSec Partners and Luis Miras, an independent security consultant, suggests that telephones are becoming popular for phishing style attacks and therefore it would be prudent to avoid their use for authentication purposes.

Email. As previously argued in Section 2.3.2 email-based authentication is unsuitable for online banking. Moreover, the susceptibility of email to phishing attacks makes them inappropriate for authentication in banking systems.

Secure authentication channels have been identified, however, they are typically inefficient and/or expensive. Accordingly new authentication mechanisms should be sought.

3.3 CAP authentication

The Chip Authentication Program (CAP) is a protocol which enables the remote authentication of bank customers using their card and associated PIN. As discussed in the previous section, access to a customer's card and PIN will enable withdrawals to be made at ATMs, therefore it seems appropriate to employ CAP technology to authenticate customers as part of the credential recovery mechanism. However, CAP is a proprietary protocol introduced by MasterCard and has yet to receive sufficient scrutiny. Since earlier research has demonstrated the weaknesses of systems introduced by the banking industry [MA10, MDAB10], the adoption of CAP should be accompanied by a thorough security review.

3.4 Financial security standards

The existence of security vulnerabilities across multiple online banking systems suggests the banking industry has failed to pay sufficient diligence to the security requirements engineering process. As a consequence online banking customers are vulnerable to financial fraud and invasions of privacy. Since individual banks cannot be relied upon to develop a suitable security standards for online banking, policy makers and industry regulators should produce such documentation. In the UK this duty could be performed by Financial Services Authority (FSA) in collaboration with the Information Commissioner's Office (ICO).

Provisions for reporting. The public-facing Internet and telephone services are insufficient for reporting vulnerabilities to banks. Firstly, these services are provided by largely unskilled personnel whom are ill-equipped to deal with the vulnerabilities reported and often respond in an inappropriate manner. Secondly, making details of attacks available to unqualified staff may result in the report being leaked and exploited, rather than dealt with. Finally, the time and resources required in reporting the vulnerabilities found in this paper were considerable. Accordingly regulators and individual banks should put more appropriate mechanisms in place.

4 Response

In accordance with responsible disclosure, the Lloyds Banking Group and the Royal Bank of Scotland Group were notified of these vulnerabilities in April 2010. Subsequently UK regulators, namely the Financial Services Authority and the Information Commissioner's Office, were notified[2]. Both banks have defended their designs as a balance between security and usability. Moreover, they insist that such fraud would be detected by their back-office monitoring and profiling tools. The effectiveness of these tools should be questioned, since the evidence gathered during this work shows that it was possible to setup a new payee and subsequently transfer £750 without intervention. At the time of writing the Lloyds Banking Group and the Royal Bank of Scotland Group are insistent that their systems offer sufficient security; despite the existence of vulnerabilities highlighted in this paper. This work is therefore being published to enable wider scrutiny from the research community, industry regulators, and the press.

5 Conclusion

This paper has shown that the online banking systems offered by the Lloyds Banking Group and the Royal Bank of Scotland Group are vulnerable to an attack which permits an adversary to commit financial fraud. The vulnerabilities have arisen as a result of poor software engineering practice by the banking industry which neglected security in favour of usability. More precisely, the banks utilise credential recovery mechanisms that are reliant on personal questions which have associated answers that are not secret between banks and customers; that is, they may be derived by an adversary. In the case of the Lloyds Banking Group, the adversary also requires access to email accounts, but as discussed, this is typically possible. In addition, the Lloyds Banking Group and the Royal Bank of Scotland Group have failed to introduce suitable technical measures to en-

---

[2]The European Central Bank have also been notified, but did not comment as this work was thought to be beyond their remit.

sure the security of personal data, thus compromising the rights of customers to financial privacy. It is believed that these vulnerabilities are not isolated to the online banking systems offered by the Lloyds Banking Group and the Royal Bank of Scotland Group, accordingly the banking industry should conduct a thorough review.

The *'liability shift'* from the banking industry to the consumer, using inadequately designed authentication mechanisms, attempts to push the cost of online banking fraud to the customer [BBG00, Mur09, MDAB10]. Indeed, the consumer rights organisation Which? reports that twenty percent of customers are not refunded after claiming to be victims of fraud [Whi09]. In some of these cases the banks may attribute blame on the basis of audit trails which suggest a customer authenticated using online banking systems. This paper questions the validity of audit trails associated with such authentication mechanisms and may help explain cases in which customers have been charged for fraudulent transactions, even when customers are adamant that they did not authorise such payments. Accordingly, it is hoped that publishing this work will prevent banks from incorrectly blaming customers for fraud in the future; helping bring an end to unfair banking practices.

References

[And10]   Jeff Anderson. Mobile Spoofing. Watchdog, BBC, 2010. Available from `http://www.bbc.co.uk/blogs/watchdog/2010/04/mobile_spoofing.html`.

[BBC08]   BBC. Palin e-mail hack details emerge. Available from `http://news.bbc.co.uk/1/hi/technology/7624809.stm`, September 2008.

[BBC09]   BBC. Twitter calls lawyer over hacking. Available from `http://news.bbc.co.uk/1/hi/8153122.stm`, July 2009.

[BBG00]   Nicholas Bohm, Ian Brown, and Brian Gladman. Electronic commerce: Who carries the risk of fraud. *Journal of Information Law and Technology*, 3, 2000.

[BJM10]   Joseph Bonneau, Mike Just, and Greg Matthews. What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions. In *FC'10: Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security*, LNCS. Springer, 2010. To appear.

[FPS07]   Jason Franklin, Vern Paxson, and Adrian Perrig Stefan Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 375–388, New York, NY, USA, 2007. ACM.

[Gar03]   Simson L. Garfinkel. Email-Based Identification and Authentication: An Alternative to PKI? *IEEE Security and Privacy*, 1(6):20–26, 2003.

[GJ05]   Virgil Griffith and Markus Jakobsson. Messinwith Texas Deriving Mothers Maiden Names Using Public Records. In *ACNS'05: Applied Cryptography and Network Security*, volume 3531 of *LNCS*, pages 91–103. Springer, 2005.

[HEF09]   Thorsten Holz, Markus Engelberth, and Felix C. Freiling. Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones. In *ESORICS*, pages 1–18, 2009.

[Hou08]   House of Commons, Justice Committee. *Protection of Private Data: First Report of Session 2007-08*. Stationery Office Books, 2008.

[JA09]   Mike Just and David Aspinall. Personal choice and challenge questions: a security and usability assessment. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–11, New York, NY, USA, 2009. ACM.

[Jus04]   Mike Just. Designing and Evaluating Challenge-Question Systems. *IEEE Security & Privacy*, 2(5):32–39, 2004.

[LM09]   Zane Lackey and Luis Miras. Attacking SMS. In *Black Hat Briefings USA*, Caesars Palace, Las Vegas, USA, 2009. See also [And10].

[MA10]   Steven J. Murdoch and Ross Anderson. Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication. In *FC'10: Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security*, LNCS. Springer, 2010. To appear.

[McK10]   Matt McKeon. The Evolution of Privacy on Facebook. Available from `http://mattmckeon.com/facebook-privacy/`, May 2010.

[MDAB10]   Steven J. Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and PIN is Broken. In *S&P'10: Proceedings of the 31st IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2010. IEEE Computer Society. To appear.

[Mur09]   Steven J. Murdoch. Reliability of Chip & PIN evidence in banking disputes. *Digital Evidence and Electronic Signature Law Review*, 6:98–115, 2009.

[MVO07]   Mohammad Mannan and Paul C. Van Oorschot. Security and Usability: The Gap in Real-World Online Banking. In *NSPW'07: Proceedings of the New Security Paradigms Workshop*, 2007.

[Ops10]   Kurt Opsahl. Facebook's Eroding Privacy Policy: A Timeline. Available from `http://www.eff.org/deeplinks/2010/04/facebook-timeline`, April 2010.

[PBH96]   John Podd, Julie Bunnell, and Ron Henderson. Cost-Effective Computer Security: Cognitive and Associative Passwords. In *OZCHI '96: Proceedings of the 6th Australian Conference on Computer-Human Interaction (OZCHI '96)*, page 304, Washington, DC, USA, 1996. IEEE Computer Society.

[Poy08]   Kieran Poynter. *Review of information security at HM Revenue and Customs: Final report*. Her Majesty's Stationery Office, 2008.

[Rab08]   Ariel Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of Facebook. In *SOUPS'08: Proceedings of the 4th symposium on Usable privacy and security*, pages 13–23, New York, NY, USA, 2008. ACM.

[SBE09]   Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. It's No Secret. Measuring the Security and Reliability of Authentication via 'Secret' Questions. In *S&P'09: Proceedings of the 30th IEEE Symposium on Security and Privacy*, pages 375–390, Washington, DC, USA, 2009. IEEE Computer Society.

[SDOF07]   Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *S&P'07: Proceedings of the IEEE Symposium on Security & Privacy*, 2007.

[Smy10]   Ben Smyth. Privacy vs. usability: A failure of barclays online banking? Technical Report CSR-10-05, School of Computer Science, University of Birmingham, 2010.

[SS10]   Ben Smyth and Chris Smith. Exploiting Natwest and RBS online banking systems for profit. Video available online at `http://www.bensmyth.com/publications/10nat/`, April 2010.

[Sym10]   Symantec. Internet security threat report. Volume 15, April 2010.

[The10]   The UK Cards Association Limited. New Card and Banking Fraud Figures. Available from `http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/`, March 2010.

[Tur10]   Stuart Turton. Barclays online banking vulnerable to snoopers. PC Pro, April 2010.

[Whi09]   Which? Fraud victims struggle to get money back: One in five financial fraud victims not reimbursed. Available from `http://www.which.co.uk/news/2009/06/fraud-victims-struggle-to-get-money-back-179150.jsp`, June 2009.

[ZH90]   Moshe Zviran and William J. Haga. User authentication by cognitive passwords: an empirical assessment. In *JCIT: Proceedings of the fifth Jerusalem conference on Information technology*, pages 137–144, Los Alamitos, CA, USA, 1990. IEEE Computer Society Press.