Using Facebook to Reset Bank Passwords

Tom Chothia, Gurchetan Singh, Ben Smyth
Univ. of Birmingham

October 1, 2010

1 Introduction

We have investigated the usability and security of online banking and found a number of shocking weaknesses. In particular, we have found that, while the main login system for the sites we looked at is secure, the "forgotten your password" systems of some banks is based on information that is easily obtainable and/or relies on unsecured e-mail. We go on to demonstrate that much of the information required to reset the online banking password of Lloyds group banks can be found by crawling Facebook.

The fundamental notion underlying the "forgotten your password" credential recovery mechanisms of banks websites is that customers cannot remember arbitrary strings; that is, customers should be assumed to forget authentication credentials. Personal questions are used to 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. In this extended abstract we point out that much of this information is not secret and can be recovered easily from Facebook.

There have been a number of papers that have looked at the security of the "forgotten your password" questions [7, 3, 5, 2, 4] and papers that have looked at the public information on Facebook [2, 1, 4]. The contribution of our work is to directly point out the weakness of some UK banks, and to show that much of this information can be found automatically by crawling Facebook. We have talked to the banks involved about our work, and it has been reported in the Sunday Times [6].

2 Lloyds Banking Group Password Recovery

Security questions used by Lloyds Group Banks (including the Bank of Scotland and Halifax) are your Father's first name, Mother's first name, Place of Birth and First school, as well as a user generated question. Quite often people frame the user-generated question in such a way that it provides no security.

An attacker must then gain access to the customer's email account to complete the authentication process, which while may be difficult in some cases is usually not secure. 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.

3 Password Reset Information on Facebook

We have investigated how much of this information is available via Facebook. Private listings on Facebook, which are only visible to friends, often include the place of birth and first school. In an unscientific survey of 100 of our

friends we found that 18 displayed this information.

Eight friends are displayed in the public listings on Facebook and these change when a user adds a new friend to his friend list or deletes an existing friend. By analysing the pattern of the change in the list shown, it was found that, on average, this leads to the list changing 4 times in a 10 day period (although, of course, this varies greatly depending on how much the user in question logs onto Facebook). This change enables us to obtain data from the modified list by running a script that crawls Facebook every few days. We did this and collected the friends, and friends of friends, of a number of volunteers. In this un-scientific sample, we found that looking for friends and friends of friends for a week, and matching surnames, would find the name of at least on parent in 13 percent of cases, with a false positive rate of 30 percent.

While crawling Facebook we found that performing hundreds of requests an hour would result in Facebook asking for captchas for future requests from that IP address. Furthermore, Facebook started blocking Tor during the course of our work. However, we also found that the Facebook captcha only checks the length of the words the user is asked for, so it can be easily brute-forced. Furthermore, only requesting tens of pages at a time does not lead to being asked for a captcha, and still makes it possible to search for the parents' names that are needed for the password reset.

Possible solutions: To make the issuing of new passwords secure, banks must move away from personal questions as authentication mechanisms. The most secure mechanism for a bank to authenticate a customer in-branch. Primarily this follows from the bank's ability to examine documentation, which supports the claimed identity of a customer. Another option would be the use of Automated Teller Machines (ATMs) to authenticate customers with respect to their smartcard and Personal Identification Number (PIN), which is a shared secret between the customer and bank.

4 Conclusion

The security questions used by banks to reset passwords are insecure and, in particular, parents' first names should not be considered secret. Users should also take care when considering if they should accept a friend request from their parents on Facebook!

References

[1] Joseph Bonneau, Jonathan Anderson, Ross Anderson, and Frank Stajano. Eight friends are enough: social graph approximation via public listings. In *SNS '09*, 2009.

[2] Mike Just and David Aspinall. Personal choice and challenge questions: a security and usability assessment. In *SOUPS '09*, 2009.

[3] John Podd, Julie Bunnell, and Ron Henderson. Cost-Effective Computer Security: Cognitive and Associative Passwords. In *OZCHI '96*, 1996.

[4] Ariel Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of facebook. In *SOUPS*, 2008.

[5] 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*, 2009.

[6] Lauren Thompson. Log-ins strengthened to thwart hackers. The Sunday Times. May 29, 2010.

[7] 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.