Privacy vs. Usability: A failure of Barclays online banking?

Ben Smyth

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

Barclays online banking system is vulnerable to a remote attack which allows an adversary to view customer bank statements and transfer money between a customer's accounts. The vulnerability has arisen as a result of poor software engineering practice which neglected security in favour of usability. More precisely, Barclays authentication mechanism is reliant on four pieces of customer data, namely: surname, date of birth, sixteen digit card number and three digit card security code (the number on the reverse of the card). This simplifies the login process for the user. However, this information is publicly available and hence it can also be used by an adversary. Barclays have therefore failed in their duty to protect the financial privacy of their customers. Moreover, the system may leave customers open to fraud and even financial loss.

1 Introduction

Security engineers endeavour to deploy systems which protect user privacy regardless of the behaviour employed by miscreants. From an online banking perspective the key privacy objective is to protect financial information from unauthorised access.

Usability experts strive to deliver systems which people can employ with ease. The key aspects of usability include learnability, efficiency and memorability. These features are desirable for online banking systems to increase user satisfaction; and from a corporate perspective, to reduce user support costs and expand the customer base.

Online banking is a domain in which the contention between these specialists can be observed; each with the conviction that the other's objective defeats their own goal. This article studies whether financial privacy should be sacrificed for usability with a focus on Barclays online banking system as a case study.

2 Online banking

Online banking is prevalent in our society due to the convenience it offers. However, the technology presents security problems for banks. In particular, traditional one-factor authentication mechanisms (for example, username and password) are deemed insufficient. This problem has been addressed in the UK by employing 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 PIN, to remotely authenticate bank customers.

1

Barclays are one such institution which utilise CAP for customer authentication on their online banking system. However, Barclays recently introduced an *'Instant Access'* service for usability reasons, this service does not use CAP nor the traditional username and password authentication mechanism. The authentication mechanism for *Instant Access*[1] requires knowledge of the following pieces of customer information:

1. Surname

2. Date of birth

3. Sixteen digit card number

4. Three digit card security code

These details should be considered public knowledge and therefore known by an adversary. It follows immediately that an attacker is able to impersonate a customer to peruse the customer's bank statements and transfer money between the customer's accounts; thus violating the goal of protecting financial information from unauthorised access.

3 Balancing requirements

The necessity for a balance between security and usability is apparent from our society. Software engineers must therefore provide adequate security mechanisms that users are comfortable with.

Financial privacy. Bank statements contain a wealth of information which should be considered private. At the very least an individual's spending patterns can be extracted; and more disconcertingly, a detailed picture of an individual's personal life can be painted by considering to whom payments have been made. Privacy in this context is generally well supported by society.

In the context of the legal system financial privacy encompasses the requirement to protect financial information from unauthorised access. Indeed, in the

---

[1]The login page needed to launch this attack is available at the following URL `https://ibank.barclays.co.uk/olb/r/MobiBasicAccessStart.do`, which is indirectly accessible from `https://www.barclays.mobi`.

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 CAP specification defines a handheld card reader which is used in conjunction with the customer's EMV smartcard and PIN to derive a one time password. This multi-factor authentication mechanism has been deemed to provide sufficient security in the context of online banking.

Usability. The CAP protocol provides enhanced security, but places a burden on the user in terms of learnability, efficiency and memorability.

Traditional one-factor authentication mechanisms require the user to recall a username and password. By comparison, Barclays implementation of the CAP protocol requires the customer to use a card reader and their EMV smartcard, in associated with the card's PIN, to compute a one time password. This password can then be used in conjunction with the customer's username, surname and last four digits of the card number to authenticate. This requires the customer to be in possession of their card reader and EMV smartcard, a requirement which is especially problematic to frequent travellers. The usability gulf between one-factor authentication and the CAP protocol should now be apparent.

Privacy vs. Usability. The perspectives of society and the legal system dictate the need for financial privacy. The CAP protocol has achieved this objective, but, the necessity for a balance between privacy and usability has been neglected.

4 A failure of Barclays?

The overheads of the CAP protocol have been identified by Barclays and an alternative *Instant Access* service has been launched. However, a remote adversary is able to exploit the authentication mechanism of the *Instant Access* service to access an individual's confidential financial information. This should be considered a security flaw because the system fails to protect privacy.

Attack feasibility. The feasibility of the attack against Barclays online banking system is dependent upon the attacker's ability to derive the four pieces of customer data we discussed earlier; namely, a customer's surname, date of birth, sixteen digit card number, and three digit card security code (the number on the reverse of the card). Hence, the availability of such data is the linchpin of the attack and the justification for considering these values as public knowledge will now be discussed. We will first distinguish three types of adversary: *insider*, *merchant*, and *outsiders*.

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

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

Outsiders have no relationship with the customer.

It is immediately apparent that insiders can trivially acquire the necessary customer information. We shall therefore focus on merchants and outsiders. 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 can also be learnt from the card, or will be supplied to the merchant for billing purposes; hence it remains to consider how the customer's date of birth can be derived. Again, this 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 pub-

lished on the Internet, in particular on social networking sites. Finally we consider outsiders whom may rely upon a variety of techniques including: dumpster diving; third party data loss (for example, those similar to the HMRC incident in 2007); and malware (in particular, keyloggers). Note that the keylogger approach is particularly worrying since it permits automated attack. It follows immediately that the vulnerability poses a real threat.

Attacks for financial gain. Primarily this is an attack against customer privacy, that is, the attack is not for financial gain. (Recall that the attacker only has the ability to view customer bank statements and transfer money between the customer's accounts; in particular, the attacker is unable to transfer money to accounts not under the customer's control.) However, we highlight two possible attack scenarios which may lead to financial gain. Firstly, the information gleaned by access to a customer's online banking account may be sufficient to launch an attack on a secondary channel; for example, using Barclays telephone banking service, or by visiting a Barclays branch in person. In addition, such information may aid identity theft. Evaluating the feasibility of these attacks remains an open question. Secondly, we consider a rather extreme scenario. Consider an unscrupulous hotelier whom takes customer bookings which require a sixteen digit card number and the three digit security code. These bookings may be made in person, online or using the telephone. When the customer arrives at the hotel they are asked to provide their passport or some form of identification (this is standard practice), which contains the customer's surname and date of birth. The hotelier is now able to view the customer's bank statements and make an informed decision to rob the guest during their stay.

Other attacks. The exploitation of the authentication mechanism allows an attacker to transfer money between a customer's accounts. This can be abused to cause financial loss and/or inconvenience. For example, a customer may be subjected to bank charges, or other penalties; loss of interest may be in-

curred; and a customer's debit card may be rejected. This attack landscape should be further explored.

5 Solutions

In accordance with responsible disclosure Barclays were notified of this vulnerability in September 2009. Barclays have defended their design as a balance between privacy and usability. Subsequently UK regulators, namely the Financial Services Authority and the Information Commissioner's Office, were notified. At the time of writing Barclays online banking system is vulnerable to attack.

Security and usability trade-off. This article has argued that financial privacy is of utmost importance. An objective which is achieved using the CAP protocol. However, this solution is particularly heavy weight and presents usability problems. Alternative security mechanisms should therefore be sought. In the context of Barclays online banking system, it should be considered whether the traditional one-factor username and password authentication mechanism is sufficient for accessing customer bank statements. The CAP protocol could be relied upon for higher risk activities, for example, transferring funds between accounts.

Financial security standards. Barclays claim the vulnerability is a design feature introduced for customer convenience. This suggests there has been a failure in the security requirements engineering process and as a consequence Barclays have neglected to protect customer privacy. Since individual banks cannot be relied upon to develop a suitable security standard for online banking, we appeal to policymakers and industry regulators to produce such documentation. In the UK this duty could be performed by Financial Services Authority in collaboration with the Information Commissioner's Office.

––––––––––

The privacy vs. usability debate is also of interest in the broader sense. As highlighted by Donald Norman, professor of design at Northwestern University, these two components may appear immutably bound in the sense that more usability implies less security; but they are in fact inherently different problems. They require an understanding of the need for protection and a comprehension of what constitutes a reasonable user effort. These are design issues and developing a suitable conceptual model in which the two can coexist is an open problem for the academic community. Online banking systems are one particular application domain which will benefit from such a framework.

A Attack history

The attack demonstrated using the URL `https://www.barclays.mobi` has been available since January 18, 2010 when Barclays launched their mobile online banking service. A variant of this attack was discovered on September 23, 2009 against Barclays standard online banking service. This attack can still be launched using the URL `https://ibank.barclays.co.uk/` and selecting the *"Personal/Premier customers: forgotten your PINsentry card reader?"* hyperlink. The vulnerability is dependent on access to the same four pieces of customer data discussed, that is, a customer's surname, date of birth, sixteen digit card number, and three digit card security code. This attack is slightly more cumbersome as the adversary is required to click-through several pages and provide a memorable word (this word may be selected arbitrarily by the adversary and hence does not provide protection against the attack).

B Update May 17, 2010

As of May 17, 2010 Barclays have removed their *'Instant Access'* service as described in this article. Thanks to Bogdan Warinschi and Mark Ryan for notification of this progress.