Exploiting Natwest and RBS online banking systems for profit

Ben Smyth and Chris Smith

School of Computer Science,
University of Birmingham, UK

Technical Report CSR-10-11

July 20, 2010
(Initial draft: April 8, 2010)

The Natwest and Royal Bank of Scotland (RBS) online banking systems are vulnerable to a remote attack which allows an adversary to steal money from a customer's account. The vulnerability has arisen as a result of poor software engineering practice which neglected security. More precisely, the authentication mechanisms used by Natwest and RBS are dependent on six pieces of customer data, namely: name, date of birth, sixteen digit card number, three digit card security code (the number on the reverse of the card), sort code and account number. This information is publicly available and hence it can also be used by an adversary. Natwest and RBS have therefore failed in their duty to protect customers from financial fraud.

1 Introduction

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 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. Natwest and RBS[1] utilise CAP for actions which they deem to be particularly sensitive. However, this article will demonstrate failures in the design process which may be exploited to commit fraud.

2 Failure of Natwest and RBS

The attack can be launched by visiting the Natwest and/or RBS online banking login page and selecting the *"Forgotten any of your log in details?"* option[2]. 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

[1] Natwest and RBS are part of the Royal Bank of Scotland Group and both use the same online banking system.

[2] The login pages needed to launch this attack are available from the URLs: `https://www.nwolb.com/onlineenrolmentregister.aspx?IsReenrolment=1` and `https://www.rbsdigital.com/onlineenrolmentregister.aspx?IsReenrolment=1`; which are indirectly accessible from `https://www.nwolb.com` and `https://www.rbsdigital.com/`.

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 the customer has previously made a payment. It follows immediately that an attacker is able to impersonate a customer to steal funds. A video demonstrating the attack is available online: `http://www.bensmyth.com/publications/10nat/`.

Poor security engineering. A fundamental difficulty in developing secure authentication systems is overcoming an inherent human weakness: the inability to recall arbitrary strings. This is overcome by Natwest and RBS using the alternative authentication mechanism which is reliant on a set of personal questions; unfortunately the answers to these questions are typically public and hence an adversary is able to impersonate a customer.

Once a customer/adversary has authenticated the following services are available:

- View statements
- Transfer money between a customer's accounts
- Transfer money to previous payees
- Apply for additional products (e.g., credit cards, loans and overdrafts)
- Cancel payments (e.g., standing orders)

In addition, a customer is able to authenticate using CAP to access services including:

- Transfer money to a new payee
- Arrange new payments
- Modify existing payments

The ability to transfer money to previous payees is a particularly sensitive service which should only accessible after additional authentication (for example, using CAP). In this respect Natwest and RBS have failed to protect customers from financial fraud.

The privacy issues surrounding improper authentication have previously been discussed[3]. 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: *"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."* Finally, the ability to cancel payments may result in charges being incurred by the customer.

Attack feasibility. The feasibility of the attack is dependent upon the adversary's ability to derive the six pieces of customer data we discussed earlier; namely, a customer's name, date of birth, sixteen digit card number, three digit card security code (the number on the reverse of the card), sort code and account number. 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, 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.

It is immediately apparent that insiders can trivially acquire the necessary customer information. We shall

[3] See `http://www.bensmyth.com/publications/10barc/`

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 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. (Note that unlike some UK banks a customer's card does not contain the account number.) Account numbers appear on cheques or may be provided for billing purposes (for example, when setting up a direct debit or standing order). 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.

Financial reward. In order to gain financially from this attack the adversary must be able to access the account to which funds were transferred. The adversary must therefore be either a *payee* of the account holder, or act in collaboration with a *payee*. The feasibility of this assumption will now be demonstrated by two examples.

First consider an ex-partner. It is of course reasonable to assume that name and date of birth will be known. Access to a debit card would also have been trivially, hence the card's sixteen digit number and security code could have been obtained. Finally, we may expect a couple to transfer money between their accounts, hence sort code and account number will be known; moreover, an ex-partner is therefore a previous payee. It follows immediately that an ex-partner may exploit the alternative authentication mechanism to steal a money.

Secondly, we consider a scenario in which the adversary acts in collaboration with a payee. The adversary may employ techniques such as bribery, blackmail or violence to gain the cooperation of the payee. In addition, the adversary must be able to utilise the alternative authentication mechanism. This can be achieved using the aforementioned techniques.

3 Solutions

In accordance with responsible disclosure Natwest and RBS were notified of this vulnerability in April 2010. Natwest and RBS have defended their design as a balance between security and usability. Moreover, they insist that such fraud would be detected by their back-office monitoring and profiling tools. However, the evidence gathered during this work suggests such tools are ineffective as it was possible to setup a new payee and subsequently transfer £750. Subsequently UK regulators, namely the Financial Services Authority and the Information Commissioner's Office, were notified. At the time of writing Natwest and RBS online banking systems are vulnerable to attack.

Guidelines for CAP usage. The CAP specification defines an authentication protocol for EMV smartcards, that is, debit cards issued by banks. The specification does not specify for which actions CAP should be utilised; although, it is implicit that it should be used for sensitive actions. However, as we have illustrated by the discovery of security vulnerabilities in online banking systems, the banking sector has failed to pay sufficient diligence in defining such sensitive actions. As a consequence online banking customers are vulnerable to financial fraud. Since individual banks cannot be relied upon to develop a suitable security standard for online banking, policy makers and industry regulators should produce guidelines for CAP usage. In the UK this duty could be performed by Financial Services Authority in collaboration with the Information Commissioner's Office.

Acknowledgements. We are particularly grateful to Zeyn Saigol for helping us test this attack.