Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication (short paper)

Steven J. Murdoch and Ross Anderson

Computer Laboratory, University of Cambridge, UK
http://www.cl.cam.ac.uk/users/{sjm217,rja14}

Abstract. Banks worldwide are starting to authenticate online card transactions using the '3-D Secure' protocol, which is branded as Verified by Visa and MasterCard SecureCode. This has been partly driven by the sharp increase in online fraud that followed the deployment of EMV smart cards for cardholder-present payments in Europe and elsewhere. 3-D Secure has so far escaped academic scrutiny; yet it might be a textbook example of how not to design an authentication protocol. It ignores good design principles and has significant vulnerabilities, some of which are already being exploited. Also, it provides a fascinating lesson in security economics. While other single sign-on schemes such as OpenID, InfoCard and Liberty came up with decent technology they got the economics wrong, and their schemes have not been adopted. 3-D Secure has lousy technology, but got the economics right (at least for banks and merchants); it now boasts hundreds of millions of accounts. We suggest a path towards more robust authentication that is technologically sound and where the economics would work for banks, merchants and customers – given a gentle regulatory nudge.

1 Introduction

Card-not-present transactions take place over the Internet, phone, or post, where the merchant and point-of-sale are not in the same physical location as the card and its holder. Fraudulent transactions of this type now account for a large proportion of bank fraud losses. In the UK, for example, it increased 118% from 2003 to 2008, when it accounted for £328.4m of losses to banks and merchants – over half the £610m total for all bank card fraud [3].

This rapid increase has been driven by the deployment of smart cards based on the EMV (Europay, MasterCard, Visa) framework [7] (branded in the English-speaking world as 'Chip & PIN'). The UK started this in 2003 and completed it around 2006; most of Europe has now finished the rollout and other countries, such as Canada, are starting. Figure 1 shows the effects on the UK fraud figures. Chips reduced fraud via lost and stolen cards, and made card counterfeiting harder for a while (until crooks learned to use the cards overseas), but card-not-present fraud rose dramatically.

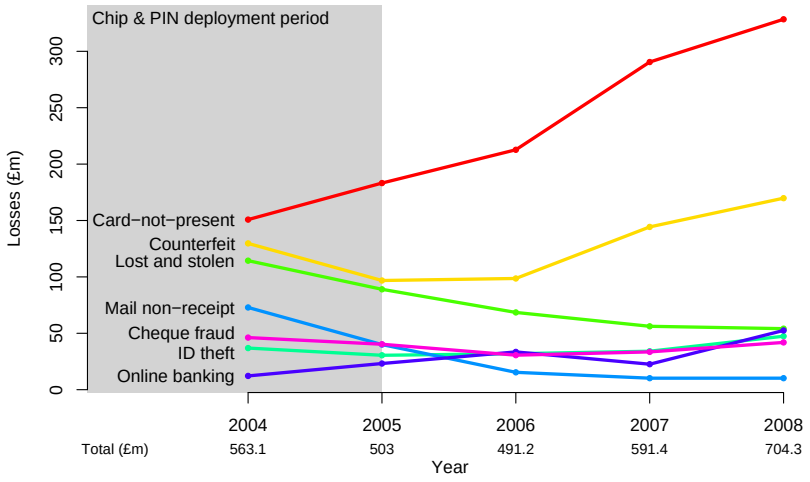

Fig. 1. Fraud totals in the UK [3].

The industry's response to this surge has been 3-D Secure (3DS), known under its brand names 'Verified by Visa' and 'MasterCard SecureCode' [1]. In its initial form, 3DS would pop up a password entry form to a bank customer who attempted an online card payment; she would enter a password and, if it was correct, would be returned to the merchant website to complete the transaction. Difficulties arose with pop-up blockers and now the recommended mode of operation uses inline-frames ('iframe'). The merchant passes the card number to Visa or Mastercard, and gets back a URL to embed in an iframe to display to the customer. If the customer executes the protocol successfully, the merchant gets an authorisation code to submit to his bank.

2 Security weaknesses

The primary purpose of 3DS is to allow a merchant to establish whether a customer controls a particular card number. It is essentially a single-sign on system, operated by Visa and MasterCard, and it differs in two main ways from existing schemes such as OpenID or InfoCard. First, its use is encouraged by contractual terms on liability: merchants who adopt 3DS have reduced liability for disputed transactions. Previous single sign-on schemes lacked liability agreements, which hampered their take-up. Few organizations are willing to trust a third-party service provider to authenticate users when they have no recourse in the event of error or attack. (In any case, security economics teaches that you're unlikely to get a secure system if Alice guards it while Bob pays the cost of failure.) Second, in other respects 3DS does not adopt the lessons learned from single-sign on, and breaks many established security rules.

2.1 Confusing the user – hiding security cues

The standard advice given to customers to prevent phishing attacks is that they should only enter their bank password in TLS secured sites, and where they have verified the domain name matches what they expect. Browsers have introduced measures to help customers, such as changing the colour of the address bar if TLS is enabled, and making it clearer who the domain name belongs to (e.g. through extended validation certificates). Because the 3DS form is an iframe or pop-up without an address bar, there is no easy way for a customer to verify who is asking for their password. This not only makes attacks against 3DS easier, but undermines other anti-phishing initiatives by contradicting previous advice (as do emails from banks containing clickable URLs). In fact, when one of the authors first encountered 3DS, he established that the iframe came from `securesuite.co.uk` and called his bank, who informed him that this was a phishing site. Actually this domain name belongs to Cyota (owned by RSA), the company to which many UK banks have outsourced the 3DS authentication process.

2.2 Activation during shopping

Before 3DS can be used to authenticate transactions, cardholders must register a password with their bank. A reasonably secure method would be to send a password to the customer's registered address, but to save money the typical bank merely solicits a password online the first time the customer shops online with a 3DS enabled card – known as activation during shopping (ADS). To confirm that the customer is the authorized cardholder, the ADS form may ask for some weak authenticators (e.g. date of birth), although not all banks do even this. From the customer's perspective, an online shopping website is asking for personal details. This further undermines customers' security usability and trust experience; and it is being exploited by criminals, as phishing websites impersonating the ADS form to ask for banking details [8] (see Figure 2).

2.3 Informed consent and password choice

By setting up a 3DS password, the customer is deemed to have accepted new terms and conditions. But ADS is not an effective way to obtain informed consent: at the time the terms and conditions are presented, the customer's primary task is to complete the online purchase, so she will not pay much attention to contract terms. Also, because setting a password is a secondary task, they are more likely to choose a poor password, or one they use elsewhere. While Visa requires that customers can opt out at least the first three times, banks may try to force 3DS activation after this stage by preventing the purchase. One of the authors attempted to opt out of using 3DS with a Maestro product; the issuer, the NatWest Bank (now majority-owned by the UK Government), did not allow even one card use without activating 3DS for the account.

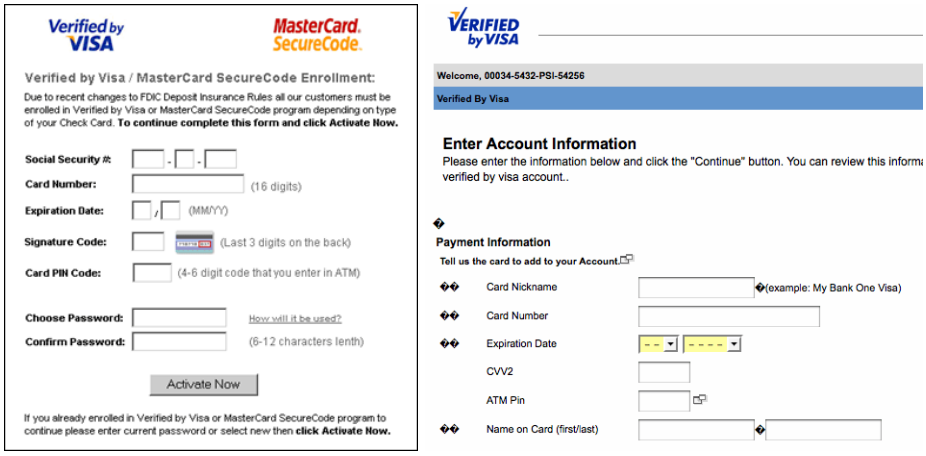

Fig. 2. Examples of phishing sites targeting 3DS.

2.4 Liability shifting

As few customers object to terms and conditions, banks are free to set terms that shift liability to customers. For example, the Royal Bank of Scotland says [2]: "You understand that you are financially responsible for all uses of RBS Secure." So despite the bank having made many poor security choices, the customer must accept the losses – a clear example of misplaced incentives. The use of passwords also harms customer interests because they no longer have the statutory protection afforded by signatures where, in the UK at least, the law makes a forged signature void and thus prevents banks from using their terms and conditions to make customers liable for forged cheques. It has already been documented that many banks used the move away from manuscript signatures to make customers liable for fraud [4].

2.5 Mutual authentication

3DS may help the customer verify that she's talking to her actual bank by displaying a memorable phrase she chooses during the ADS process. But first, customers are unlikely to choose a good phrase, given that their goal during ADS is not security but shopping; and second, the memorable phrase is trivially vulnerable to a man-in-the-middle attack.

2.6 Inconsistent authentication methods

The 3DS specification only covers the communication between the merchant, issuer, acquirer and payment scheme, not how customer verification is performed. This is left to the issuer, and some have made extremely unwise choices. For instance, one bank asks for the cardholder's ATM PIN. It's bad enough that EMV

has trained cardholders to enter ATM PINs at terminals in shops; training them to enter PINs at random e-commerce sites is just grossly negligent. (Phishermen are also asking for ATM PINs on bogus ADS forms.)

Another issuer-specific choice is how to reset the password when a customer forgets it; here again corners are cut. Some banks respond to one or two failed password attempts by prompting an online password reset using essentially the same mechanisms as ADS. In a number of cases the bank requires only the cardholder's date of birth, which is easily available from public records; with one (UK-government-owned) bank, two wrong password attempts simply lead to an invitation to set a new password.

A third variable factor is whether the 3DS implementation asks for a whole password or for some subset of its letters. The idea behind asking for a subset is that a single-round keyboard logging attack does not compromise the whole password. However this compels users to select relatively simple passwords, and probably to write them down. (Thereby they will be in breach of the bank's terms and conditions, and can be refused a refund in case of fraud; so asking for a subset may actually be a rational design choice for the bank.)

2.7 Privacy

An early single sign-on system (Microsoft Passport) was criticised on privacy grounds; modern technologies such as Credentica's U-Prove (being built into the Microsoft InfoCard framework) prevent customers being profiled, even by their authentication provider. 3DS, by contrast, requires that for the cardholder to be shown a description of the transaction, this must be sent to the issuer.

With interbank payment systems, the issuer is told which merchant the customer is dealing with, but the online payment protocol SET (Secure Electronic Transactions) at least arranged things so that the merchant and the bank each got only the transaction data they needed; the bank did not get a description of the goods. So 3DS provides less privacy than either the SET proposal or the existing legacy systems. Furthermore, most banks outsource 3DS authentication and their contractors (e.g. Cyota) see detailed information on more transactions than any individual bank. As these contractors are vulnerable to compulsion (e.g. by FBI National Security Letters), the same tension may arise between U.S. 'anti-terror' law and European privacy law as arose with SWIFT.

3 The way forward

3-D Secure has received little public scrutiny despite the fact that with 250 million users of Verified by Visa alone, it's probably the largest single sign-on system ever deployed. What's more, Visa is introducing 'original credits', a payment system based on it, that can support person-to-person money transfer [9]; and EU banks are about to start implementing the Single European Payment Area E-mandate, which will work somewhat like 3DS (a customer will fill out a

bank transfer form at a supplier's website, but using her e-banking password). So it's important to understand what's wrong with 3DS, and how to fix it.

This paper has shown that while previous systems, such as InfoCard and OpenID, had good engineering, they had no incentives for adoption. 3DS fixes the economics, at least for merchants and banks: merchants who adopt it get transactions treated as cardholder-present transactions with much less risk of repudiation, while banks get to shift liability in turn to customers. (In fact the '3D' stands for three domains – the bank, the merchant and the payment network; the customer seems not to have been considered at design time.) Visa's marketing emphasises VbV's 'global liability shift' and claims that it 'addresses' 73% of merchant chargebacks [9].

But 3DS ignores the other lessons learnt from earlier systems. The result is that customers receive little benefit in security, while suffering a huge increase in their liability for fraud. They are also trained in unsafe behaviour online. Now our experience in recent years is that when attacks can be profitably industrialised, they will be; the growth of man-in-the-middle attacks and malware will ensure that 3DS is not sustainable in its present form.

What should be done technically? We believe that single sign-on is the wrong model. What's needed is transaction authentication. The system should ask the customer, "You're about to pay $X to merchant Y. If this is OK, enter the auth code". This could be added to 3DS using SMS messaging, or systems like Cronto [5] or CAP (Chip Authentication Program) [6] as a stopgap. In the long term we need to move to a trustworthy payment device. This is not rocket science; rather than spending $10 per customer to issue CAP calculators, banks should spend $20 to issue a similar device but with a USB interface and a trustworthy display.

What must be done to make it happen? As this paper should bring home, incentives are the key. Visa and MasterCard have managed to get 3DS deployed by arranging so that merchants and banks benefit (at least in the short term) while consumers lose out. What's needed now is for regulators to intervene on behalf of the consumer. The EU already has the Electronic Signature Directive, which contemplates shifting the liability for electronic transactions to bank customers if they are equipped with a secure electronic signature creation device. The missing word is 'only'. If the liability shift is permitted only once the technology actually empowers the customer to decide what transactions she will authorise, then the incentives will line up and finally we might start to move toward a sustainable infrastructure for cardholder-not-present payments.

Acknowledgements

We thank the anonymous reviewers for their comments, Saar Drimer for his contributions to discussions, and John Henderson for his description of the SEPA E-mandate system. Steven Murdoch is funded by the Tor Project and employed part-time by Cronto Ltd.

References

1. 3-D Secure system overview. https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=119.
2. RBS Secure Terms of Use, December 2009. https://www.rbssecure.co.uk/rbs/tdsecure/terms_of_use.jsp.
3. APACS. 2008 fraud figures announced by APACS, March 2009. http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/.
4. Nicholas Bohm, Ian Brown, and Brian Gladman. Electronic commerce: Who carries the risk of fraud? *The Journal of Information, Law and Technology*, (3), Oct 2000.
5. Cronto. http://www.cronto.com/download/Cronto_Products_Datasheet.pdf.
6. Saar Drimer, Steven J. Murdoch, and Ross Anderson. Optimised to fail: Card readers for online banking. In *Financial Cryptography*, LNCS 5628. Springer, 2009.
7. EMVCo, LLC. *EMV 4.1*, June 2004. http://www.emvco.com/.
8. Internet Retailer. Verified by Visa security program used as bait in phishing scams, 6 January 2005. http://www.internetretailer.com/dailyNews.asp?id=13764.
9. Jon Varco. Verified by Visa update. http://www.barclaycardbusiness.co.uk/information_zone/customer_forum/pdf/1315_jon_varco_visa.pdf.