Phish and Chips

We're with Bill Gates: we'll never fix this problem without smart cards

by

Dave Birch mailto:dave.birch@chyp.com
Steve Pannifer mailto:steve.pannifer@chyp.com

Consult Hyperion http://www.chyp.com

Four years ago, Bill Gates said that passwords were the weak link in Internet security, and that the industry needed to move to smart cards. Since then, nothing much has happened. But the latest Internet scam craze, known as "phishing" may tip the balance.

This draft 8 July 2004, 3502words (10 pages)

REAL PROBLEM, REAL MONEY

You can't have failed to notice reports of a major Internet crime wave underway on both sides of the Atlantic at the moment: *phishing*. This means duping consumers into divulging financial information using spoof web sites [1]. In non-cool, un-hacker terms, the fishing involves sending out spam e-mails to try and tempt unwary consumers into visiting the fraudsters web sites.

Every single Internet user in Britain must have received one by now. You know the form: *hello, this is Barclays* (or Citibank, or Paypal, or whoever) *and we're just checking* (or testing, or upgrading, or whatever) *our security system, so please click on this link and enter your username and password* (or card number and PIN, or whatever).

The link is, of course, not to the bank but to the fraudsters' web site. Once the customer enters their details, the fraudsters whisk them away for their own use: this use generally being to loot the bank account as quickly as possible.

Phishing works because if the fraudsters send out 10 million e-mails, and 1 in a 100 of the hapless recipients is a (for example) Citibank customer, and 1 in a 100 of them is fooled by the e-mail, that means that the fraudster could gain access to a hundred Citibank accounts. And they do. In the UK, Lloyds TSB, NatWest and Barclays have all admitted that customer accounts

have been accessed and that money has been stolen but none of them would give a figure. APACS say that they think the figure is over a million and still growing [2].

The money stolen isn't the only cost to the banks. In addition to making good that money, banks have to pay to repair the damage: changing names and passwords, re-issuing cards, reassuring customers and so on. This has already cost some £60m in the UK [3] and, according to research company Gartner, more than a billion dollars in the US last year [4].

It's a no-brainer for the bad guys. When the police in Taiwan arrested a member of an organised phishing gang (who had been targeting five local banks with a "Trojan horse" attack) they found 45 million e-mail addresses and 200,000 passwords [5]. Assuming they were average fraudsters, this means a password harvest of around half a percent is a good figure to work on. It isn't only about passwords, of course. According to *The Nilson Report*, a respected industry newsletter, a list of 200 million e-mail addresses can be purchased for €20 or so and (of that fraction of the 200 million who are actually customers of the "target" institution, in fact around 7% give up data of sufficient value to be used or sold on). No wonder it's on the rise.

SOMETHING MUST BE DONE (REALLY)

It sounds incredible that people would fall for phishing scams in such numbers, but the sophistication of the attacks is high and growing. In some cases, victims are directed to the real bank web site while a pop-up window is overlaid to capture details. In other cases, the surfer's toolbar is taken over.

One of the latest attacks against Barclays goes even further [6]. It involves tricking people into going to a web site that sneakily downloads a trojan horse programme to their PC. The trojan horse (which has been written specifically to attack Barclays' customers) watches keystrokes and thus snaffles the customer's identifier and passcode. Because Barclays' log-in then asks customers to enter two letters from a secret word, by choosing them from pop-up menu to defeat key loggers, the fraudster's software takes a picture of the screen and mails it back to them!

Attacks of this sophistication are spreading. One of the more recent efforts, known as "img1big.gif" is a Trojan horse programmed to target 50 international banks (including Citibank, who are the number one phishing target worldwide at the time of writing, accounting for about a third of all attacks in May 2004 [7]). Like many other similar Trojans, it exploits flaws in Microsoft's *Internet Explorer* web browser to surreptitiously sneak software (in this case a programme to capture usernames and passwords together with a companion installer) on to the victims' computers [8].

This isn't just about hype and media sensationalism, it's about a real, growing and highly pernicious problem. Banks can look after themselves, but if phishing continues it could well undermine the confidence of the general public in online transactions of all kinds: not just online banking, but online business and online government as a whole.

What is to be done? Phishing is possible because authentication to online services is so univerally weak, consisting of various PINs and secret phrases all of which amount to nothing

more than basic password authentication [9]. As well as this customer authentication being weak, service provider authentication is similarly weak. The very fact that phishing sites work at all proves that the authentication of banking and other e-commerce web sites is effectively non-existent: the fact is that customers need to have as much assurance that they know who they're dealing with as the service provider does about who is logging onto its service.

Against this, it is not enough to assume that customers can be educated and then relied on to recognise fraud when it happens. Warnings are all well and good, but it's just impossible to stop this sort of attack (as in the case of so many other Internet attacks) without better authentication. As Bill Gates said back in 2000 [10], and we've been saying for over a decade (eg, [11]), passwords are the weak link in Internet security and the industry needs to move to smart cards.

PHISH AND CHIPS

But who will provide authentication based on smart cards? In the UK, banks are currently spending hundreds of millions of pounds on just such a better authentication scheme: chip and PIN. As the advertisements ("Security in Numbers") have made clear, chip and PIN is targeted at shops in the real world. But suppose it could be used with your PC, TV or phone as well? And what's more, suppose it could be used without having to have a smart card reader in your PC, TV or phone? That would be a really useful immediate defence against the phishing menace [12].

As is happens, the UK Association for Payment and Clearing Services (APACS: the "club" where banks get together to sort out payments issues) have been developing the specifications[1] for such a solution: it goes by the name of "token authentication" [13]. The idea is that your bank would give you a small device, a bit like a pocket calculator (as shown in Figure 1). When you want to log in to your bank on the Internet, the bank asks you for a code number: let's call it the *response*. You put your bank card into the calculator and punch in your PIN: the device displays a code number (the response) which you then enter in to the web site or tell the person on the phone. From this number, the bank knows that you had a real card and entered the right PIN. Since you have to have both the card and the PIN in order to log in, this is known as a "two factor" authentication (as opposed to the "one factor" password).

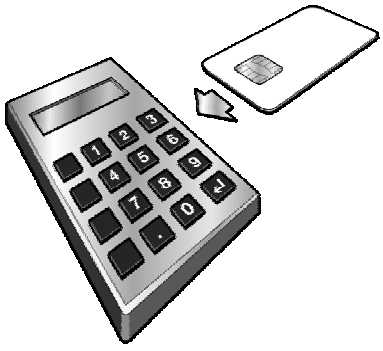

Figure 1. Token Authentication Device.

[1] Consult Hyperion were chosen by APACS to develop these specifications.

The calculator device is dumb, and therefore cheap. It doesn't do any security or cryptographic operations: these are all done in the card itself. The combination of an inexpensive and non-personalised device (in other words, you can use your card in anyone's calculator) is very attractive, which is why Barclays began a 5,000 pilot scheme with MasterCard earlier in the year [14].

The token authentication device can also work in another mode of operation. In this mode, the bank sends the customer a number: let's call it the *challenge*. The customer punches this challenge into their device and then enters their PIN. Another code number (the *challenge-response*) displayed then depends on both the PIN and the number sent from the bank, not the PIN alone. If the challenge from the bank is dependent on the transaction details specific to a transaction[2] then by sending back the displayed challenge-response the customer is in effect providing a digital signature for the transaction.

Interestingly, this usage mode also provides a means for the customer to be certain that they are talking to the bank. Just as the bank can send a challenge to the customer and check the response, so a customer can send a challenge to the bank and check their response. Here's a practical example:

- Fred gets a phone call: "Hello, this is JumboBank calling about your Super Premium Saver Plus account. Can you give me your mother's maiden name".
- Fred, being a suspicious person who has read lots phishing stories in the newspaper says "Who the hell are you? Why should I tell you my mother's maiden name? I challenge you".
- Fred, who already has his debit card inserted in his token authentication device presses a button and it displays a number[3] which Fred punches into the phone.
- JumboBank customer representative says "Our response is 976324".
- Fred punches in 976324. The device says "OK", or whatever, and now Fred knows that it really is JumboBank and can relax and listen to the customer representative who tells him about the new Super Gold Platinum Extra savings account which pays 0.15% gross per annum.

Note that the same process could be used to authenticate between any customer and service provider: someone logging on to the Inland Revenue, as an obvious example. The bank always has to be in the loop (because only the bank has the relevant security keys) and therefore can always charge for the service. Not only a way of defeating phishers and doing away with secret words, but a way of generating additional revenue.

In summary, then, using the EMV cards already issued to customers plus a simple, dumb, calculator-like device (which contains no clever cryptography, remember, as that's all on the

[2] For the technically minded, the code is formed from a "message digest" of the transaction.
[3] For the technically minded, this number is actually a transaction counter from the device.

card), customers can be sure they're dealing with their bank and banks can be sure that they're dealing with their customer.

THIRD WAY

Well, almost. This kind of authentication is a major step forward, but it still would not protect against a particular class of very sophisticated attacker who manages to sit between the customer and the service provider (eg, through cross site scripting) and at an appropriate moment (ie, after the authentication has taken place) takes over the session and empties the customer's bank account. So, the customer is connected to the bank, but a fraudster (the man-in-the-middle, as shown in Figure 2) has hijacked the connection and can change any data going from the bank to consumer or vice versa.

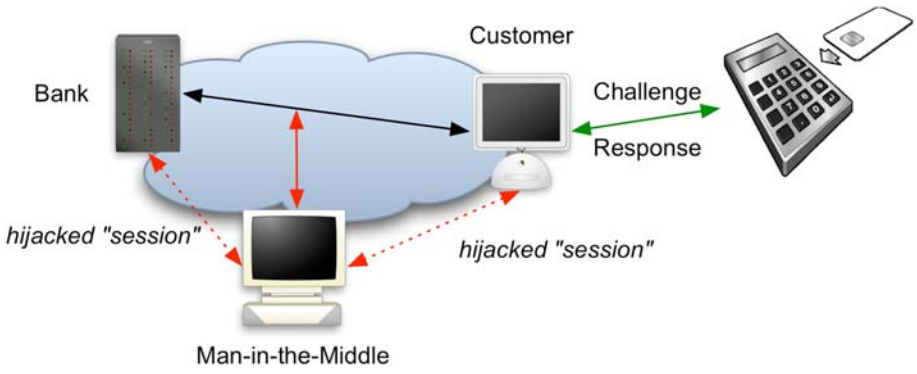

Figure 2. The Man-in-the-Middle.

The weakeness exists because an attacker can read the challenge from the bank and the response or challenge-response from the customer. They can then use these in nefarious ways. Here's an example to explain how:

- Fred connects to (he thinks) his bank. He's actually connected to Zog, a sneaky man-in-the-middle. Zog connects to the bank.
- The bank says "Hello Fred, what is your response"? Zog passes this message on to Fred.
- Fred punches in his PIN and then enters the response.
- Zog gives the bank the response. The bank thinks the response (which is the correct response, as it came from Fred's device) came from Fred.
- Zog sends a message back to Fred saying "Sorry, online banking is down for maintenance and will be back up in a few minutes".
- Zog then transfers all of Fred's money to an account in Mozambique, or wherever.

Now, the proper solution to this kind of problem (as, frankly, is well-known and well-understood) is to use Public Key Infrastructure (PKI, about which more later) but absent PKI

and trying to re-use existing infrastructure, how could token authentication defend against this kind of attack? The answer rests on the bank being able to get the challenge to the customer so that the man-in-the-middle can't read it or change it. Otherwise, you get this problem:

- Fred asks his online bank to "Transfer £1,000 to his son in London".
- Zog intercepts Fred's message and changes it to "Transfer £1,000 to Zog in Albania". The bank constructs a challenge based on the phoney transaction, not the real one (which never reached it).
- Zog sends the challenge to Fred. Fred enters the challenge and PIN and sends back the challenge-response. Zog passes this on to the bank.
- The bank now executes Zog's transaction, for which it has the correct challenge-response.

Suppose, however, that the bank could send the transaction details and associated challenge so that Zog does not see them. There are two possibilities:

- The transaction details and challenge can be sent out-of-band. The transparently obvious way to do this is via SMS, assuming that the bank knows Fred's mobile phone number.
- The transaction details can be sent in-band but (since there's no cryptography) cleverly disguised.

So far as sending in-band is concerned, there is an interesting way to do this: the machine-unreadable detail display (MUDD). Based on the same techniques widely used by online services (eg, Hotmail) to prevent machine enrollment, the MUDD converts text into a distorted graphic image that can be easily understood by a person but is fantastically difficult to interpret by a computer, An example is shown Figure 3.

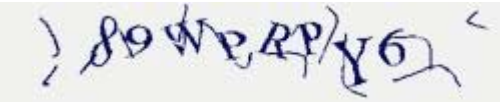

Figure 3. A Machine-Unreadable Text (89WPRPY6).

Thus, the message that the bank sends to Fred includes both the key transaction details "Son: £1000" and the challenge "123678" as a **graphic**: a MUDD, in fact. Even if Zog intercepts this message, he has to manually read it, understand it and then construct an alternative with the phoney transaction details in to send to Fred. He can still do this, of course, but now the process requires manual intervention. And this tilts the balance back in favour of the bank and Fred.

PRACTICAL DEPLOYMENT

How could such as scheme (ie, token authentication without or without MUDDs) be introduced and operated? It would be helpful to find a way that does not need banks and merchants to

create a new scheme from scratch but that could re-use existing infrastructure for authenticating customers directly with the bank.

Rather usefully, banks and merchants have begun to put just such an infrastructure in place already. It's called 3D Secure, and was originally intended to prevent credit card fraud on the Internet. When a customer who is registered for 3D Secure buys something from a 3D Secure merchant, they are connected to their bank and have to enter a password (known only by the bank, obviously) thus authenticating themselves. So, if someone steals your credit card number, it's no good to them (once all merchants are 3D Secure, naturally) without the password,

It's true that 3D Secure, marketed under the brands *Verified By Visa* and MasterCard *SecureCode*, faces a number of barriers to widespread adoption and is far from having solved the online payment fraud problem [15], but it is also fair to observe that it does actually work. Thus, it would be straightforward to get customers to enter their challenge-response instead of a 3D Secure password: all of the 3D Secure infrastructure would work as currently deployed and the merchants would not have to do anything (a big plus point). MasterCard and Visa have already developed specification to do just this.

A practical deployment is, then, to use both customer authentication and transaction signing wholly integrated into a 3D secure framework, using both modes of token operation for appropriate purposes, and incorporating the MUDD. For example

- The customer logs in to their bank account. The 3D Secure window pops up and the customer is asked for a challenge-response. They put their card into their device, enter the challenge and their PIN, and then type the displayed challenge-response into the web page.
- The customer can then check their account, pay bills and so forth with no further authentication.
- If the customer instructs the bank the transfer money to a third party, the 3D Secure window comes up again and the bank displays the transaction details and challenge as a MUDD, as shown in Figure 4,

Figure 4. 3D Secure and Token Authentication Signing.

This sounds like a bit of effort—punching in numbers and looking at the results—but it (critically) does not depend on the consumer remembering anything but their PIN: no password, no personal phrases, no secret words and no usernames. In future, the device functionality could be built in to keyboard, TV controls and even two-slot mobile phones[4] thus making it even easier to use.

It's an interesting way forward and one that deserves more attention. If you had to use your debit or credit card and PIN to log in to your bank account or to make a payment on the Internet, phishing would cease to be a threat because the phishers would need to break in and steal your card: just knowing account numbers wouldn't help them. This is the significant advantage of two-factor authentication. In fact, and we just can't resist the pun, if the industry adopted hardware-based two-factor authentication (bringing together the investments already made in EMV and 3D Secure) then the phishers would have had their chips.

IT'S A PHIX

Using EMV cards in this way provides an excellent short-term fix to phishing and related problems, but in the longer term the industry needs to move to PKI. This ought not to be complicated: apart from any else, almost all web server and web browsers implement a protocol called SSLv3 for mutual authentication using PKI. The practical exploitation of this infrastructure, however, depends on the distribution of smart cards with PKI applications on them and readers to connect them to PCs.

Going down the PKI route, it doesn't matter if Fred's messages are intercepted by Zog since they can't be decrypted, and it doesn't matter if Zog knows Fred's public key because (since Zog

[4] Remember them!

doesn't have the corresponding private key) Zog can't masquerade as Fred. Any message to Fred could only be decoded by someone with Fred's smart card and PIN.

But why go to the expense of distributing new smart cards to customers? The banks are already sending them smart cards. It just that they've chosen (in the UK, at least) to distribute smart cards that have only the EMV application on them (because they're cheaper). They could just as easily distribute smart cards with both EMV and PKI on them (American Express, in fact, have done just that with some of their *Blue* cards) and fix the Internet authentication problem once and for all.

ACKNOWLEDGEMENTS

Many thanks are due to my colleagues Neil McEvoy and Richard Allen, who were amongst the principal architects of the APACS token authentication scheme, for their insights into the practical combination of token authentication and 3D Secure technologies.

REFERENCES

1. Anderiesz, M. *A big catch in the phishing season* in *The Guardian* (*Online* section) (29th Jan. 2004).

2. Greenwood, L. *E-mail scams costs banks £1m* in *BBC News* (24th Apr. 2004).

3. Warren, P. *£60m bill for banks as online phishing hooks the unwary* in *The Evening Standard* (29th Apr. 2004).

4. *Gartner Study Finds Significant Increase in E-Mail Phishing Attacks Against U.S. Online Consumers* in *Business Wire* (6th May 2004).

5. *Taiwan hacker Targeted Banks's Online Services* in *China Daily* (5th Jul. 2004).

6. *New "Purchase Confirmation" Trojan Variant* at <http://spamwatch.codefish.net.au/> (on 10th Apr. 2004).

7. *Phishing Attack Trends Report*. Anti-Phishing Working Group, Report (San Francisco: May 2004).

8. Lemos, R. *Renegade program stealing passwords at banking sites* in *CNET News.com* (30th Jun. 2004).

9. Birch, D. *Is the end in sight for passwords?* in *Card Technology*. **8**(14): p. 18-19 (Dec. 2003).

10. Wagner, A. *Gates pushes smart card technology* in *Nando Times* (10th May 2000).

11. Birch, D. *Downloading Software, Uploading Money—Business on the Infobahn* in proc. of *Internet and the Enterprise*, Technology Appraisals (London: 1994)

12. Birch, D. *Have the phishers had their chips?* in *The Guardian* (*Online* section) (30th Jun. 2004).

13. Findlayson, P. *Token Authentication* in proc. of *5th Annual Digital Identity Forum*, Consult Hyperion (London: Nov. 2003)

14. Kotadia, M. *Barclaycard fights phishers with password generator* in *ZDNet UK* (5th Jul. 2004).

15. Litan, A. *Fighting Identity Theft and Consumer Fraud* in proc. of *ASROC*, (London: Oct. 2003)