

The Future of Phishing

Dr. Jonathan Tuliani is UK Technical Manager for Cryptomathic Ltd. In this article he examines how attackers are likely to respond to the current move towards 2-factor authentication as a defence against phishing scams, and describes an alternative approach, available today, that provides a longer-term solution.

In recent months, newspaper and television reports have highlighted how highly-organised criminal gangs are launching large-scale, carefully planned attacks against high-street banks and other services, both in the UK and overseas. These so-called ‘phishing’ attacks begin with an email. Appearing to come from the bank, it leads the recipient to a convincing web page, at which point he is tricked into entering his username and password.

Of course the web page has been set up by the attacker and does not belong to the bank at all. Once obtained, these details are used by the attacker to log in to the user’s account and drain it of funds.

Surely, in an ideal world the user would realise that the web page is bogus – that’s what SSL/TLS is all about, right? Unfortunately, a combination of browser flaws, DNS attacks, lack of control over root SSL certificates and the need to make systems user-friendly means that for most users, detecting a fraudulent web page is nigh-on impossible. Moreover, the economics of spam require that only a very small percentage of users need to fall for the scam for it to be worthwhile.

The current industry trend to counter this threat is the introduction of stronger user authentication. For reasons of cost, mobility, ease of deployment and user acceptance, password-generating tokens are the most commonly adopted technology. They supply the user with a *one-time-password*, a random string of letters or digits valid only for a single use. The idea is that the attacker is thwarted since the one-time-password, once obtained, has already been used or has expired.

Password-generating tokens are offered by a variety of vendors. The password is generated cryptographically based on a key shared with the bank, and varied either by means of a clock, a counter value or a user-input challenge – perhaps even a combination of the three. The key may be internal to the token or a separate card and reader may be used¹.

The history of security teaches us that it would be wrong to assume that the introduction of two-factor authentication will be the end of the story. Faced with additional security measures, we must assume that the attacks will evolve, and more advanced exploitations will emerge. What might these be, and how might we prepare for or respond to them?

¹ MasterCard has devised a scheme based on existing retail banking EMV chip-cards and PINs, which has been adapted in the UK by the Association of Payment Clearing Services (APACS).



My firm belief is that the next few years will see the emergence of internet man-in-the-middle attacks. Here, the user is tricked exactly as described above, except that instead of just the user communicating with the attacker, the attacker is also communicating in real-time with the bank. Two (or even ten) factor authentication is of no help, since the attacker does not interfere with the log-in process. Both the user and the bank are unaware of the presence of the attacker, and believe they have a secure connection directly from one to the other.

Once established, the man-in-the-middle has complete control. He can modify instructions, for example transferring funds to a different account to that specified by the user or simply cut the user off and submit whatever instructions he desires directly to the bank.

To combat this threat, it is necessary to move away from session-based security (based on a secure log-in), to message-based security (based on explicit authentication of individual transactions). Indeed, the password tokens mentioned above frequently permit the authentication of individual transactions. However, the man-in-the-middle is still able to substitute false transactions for authorisation, unbeknownst to the user, since the authorisation process is typically based on a 'challenge' derived from the transaction and not the explicit transaction details themselves. Whilst offering a very useful interim defence against current attacks, in the longer term an alternative approach will be required².

Several vendors already offer the option of one-time-password distribution via SMS as a cost-effective alternative to password-generating tokens. Whilst it is neither authenticated nor encrypted, it is in practice infeasible for an attacker to compromise both the SSL/TLS channel *and* the SMS channel to a particular user simultaneously. This independent channel also offers a way around the man-in-the-middle.

In the proposed scenario, the user would log in using his username and password, exactly as he does today. For each transaction entered, a summary would be returned to the user together with a one-time-password as an SMS. For example, 'Pay £50 to British Gas a/c 12345? Confirm: ADJPEQ'. Any tampering with the transaction details would be evident at this point. Assuming all is correct, the user enters the one-time-password into his PC to confirm the transaction.

As well as thwarting man-in-the-middle attacks, this approach defends against another significant emerging threat, namely malicious 'Trojans' on the user's PC. Apart from being used in direct attacks, a user may claim infection in an attempt to repudiate a legitimate transaction. The mobile phone is a separate user interface, independent of the (possibly infected) PC, thereby effectively closing this vulnerability.

Adoption of SMS-based security measures must be carefully managed, particularly the procedures used for registering and maintaining records of users' mobile phone numbers. The benefits, however, are great: there is no other cost-effective system

² MasterCard are already considering allowing the transactions details to be entered into the card reader instead of using a derived challenge, thus authenticating the transaction explicitly. This is similar to proprietary token-based schemes already offered by several vendors. However, this requires additional efforts from the user (including great scope for user error) and offers very little future flexibility, as the tokens, once issued, cannot be changed.

offering defence against phishing, man-in-the-middle and Trojan attacks whilst maintaining a simple and intuitive user experience.

Jonathan Tuliani

