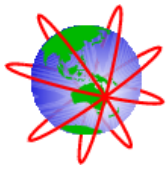

AusCERT

Australia's National Computer Emergency Response Team

EFT Code Review

Submission to ASIC

30 April 2007

Summary

AusCERT's advice and recommendations relate to liability issues surrounding the EFT code (Section 7, Part A of the discussion paper).

Please note that while the advice provided in this paper is directed specifically to the EFT Code and discussion points raised in the EFT review's discussion paper, the issues raised by AusCERT in relation to most of the malware and phishing attacks are also equally relevant to other e-commerce and e-government entities and users. Hence it is important to note these issues do not solely relate to financial institutions or their online account users.

About AusCERT

In providing the advice and recommendations in this submission, AusCERT does so from its experience and expertise as the national CERT (computer emergency response team) for Australia. In particular, AusCERT has been at the forefront of monitoring, analysing and responding to online ID theft attacks in Australia since March 2003. This involves analysing the technical features of phishing and trojan hosting sites and malware used for financial fraud and identity theft and seeking the closure of such sites in Australia and overseas.

AusCERT is an independent, non-government, not-for-profit organisation that supports the Australian public interest by helping to protect the security of the Australian Internet using community, primarily by:

- Monitoring, analysing and providing advice about computer network threats and vulnerabilities;
- Providing assistance to Australian networks facing cyber attack sourced from within Australia, or more often, overseas;
- Providing assistance to Australian law enforcement in cyber crime investigations; and
- Providing advice on how to protect against and recover from computer security attacks.

Q28

AusCERT would not support any major change to the current liability arrangements of the code and in particular where liability arising from losses resulting from vulnerability of user's equipment.

In the same way that no liability currently extends to account users for unauthorised transactions when any component of an access method is 'forged, faulty, expired or cancelled' (s 5.B.5.2 (b)), then nor should liability extend to the vulnerability or insecurity of the user's computer.

The user computer is simply an extension of the access method. Mainstream operating systems were never designed for secure transactions. The operating systems on account users' computers are highly vulnerable to attack and so too are single factor authentication (username and password) and some forms of two-factor authentication. Moreover, these systems continue to be targeted often and aggressively by online criminals.

Liability for losses resulting from vulnerability of user's equipment

With regard to claims (paragraph 7.17 of the EFT Code Review Discussion paper) that some industry representatives want to re-examine how liability for unauthorised transactions is allocated in light of the growth of fraud in the online environment and who argue that account users need to do more to reduce the risks and losses associated with online fraud, AusCERT would like to offer the following comments:

- Account holders are not responsible for the growth in fraud in the online environment – they are largely the target of such attacks.

- Financial institutions and e-business and e-government in general have encouraged, and continue to encourage users to move to the online environment to conduct various value based transactions.

- Therefore, it is largely inappropriate to transfer the risk to account holders for circumstances which are largely beyond their control. The one exception might be where a user deliberately and repeatedly refuses to take responsibility for online activity and behaviour and uses the EFT Code as the safety net. Ultimately the EFT Code should not be used to promote and reward irresponsible activity and behaviour and the financial institution should have the ability to disallow such a person from accessing the channel without challenge.

- In particular, AusCERT assesses that the volume and sophistication of online malware and (deception-based) phishing attacks are such that it is difficult to reliably eliminate the risk solely from the account holder perspective. The type of malware which is currently in widespread use has functionality far more sophisticated and harmful than has been described in this discussion paper.[1] As such it is equally inappropriate that the account user bears the total liability for protecting the online channel – and hence their cash assets.

[1] For example, see Haxdoor – an anatomy of an ID theft attack using malware, available at: https://www.auscert.org.au/7069, December 2006

- AusCERT assesses that in the face of such sophisticated and complex on-line attacks, financial institutions are better placed to reduce the insecurity of the online channel and to detect potential unauthorised transactions when they occur and take mitigation action to minimise the risk of fraud subsequently occurring than account users. The skills, resources and expertise required of users to substantially reduce the risk to their computers and by extension, their online accounts are substantial per individual or household. Furthermore, in many cases it will be impractical or not achievable, including where, for example, the user's equipment (computer) is not their own, such as a friend's or that which is a public-use Internet connected computer such as a cyber café, business lounge or library. In these cases, the account user has no capacity to reduce the vulnerability of the equipment or know what state it is in prior to use.

With regard paragraph 7.19 of the EFT Code Review Discussion paper:

> *It is generally agreed that the insecurity of end-user equipment is a major source of vulnerability to malicious software installation, and that a properly secured PC or other equipment is one of the best defences currently available against malicious code installation.*

While AusCERT agrees with this statement in principle, it does not necessarily follow that the substantive liability allocation should be shifted to account users for the following reasons:

1. It cannot be automatically assumed that account users, in general, have the skills, expertise and resources to access, purchase or maintain a "properly secured PC or other equipment". Doing so is not trivial and extends well beyond the current expectation of the EFT code that users only have to protect their access code (as detailed in s 5.6).

2. For the purposes of allocating liability, determining a minimum set of security precautions is in itself problematic as in most cases, the nature of the current threat (attack modus operandi) is such that there are generally ways of circumventing such counter-measures. Indeed it is no longer uncommon for counter-measures to subverted even when a user has adopt the following common good-practice counter-measures:

    a. Up to date operating system and application patches

    b. Up to date anti-virus and spyware applications

    c. Up to date and correctly configured firewall

    d. Use of anti-spam filters

3. AusCERT assesses that all these counter-measures are essential, but, are not by themselves sufficient to fully mitigate the risk to online account users from the type of attacks which may result in unauthorised transactions from their accounts.

4. Although AusCERT has developed its own recommended set of minimum security counter-measures[2] to reduce the risk of malware infection (which extends beyond the list described above) – this will not eliminate the risk and therefore, it is not appropriate to expect account user bear 100% of the loss of unauthorised transaction. The reality is that for many account users these minimum security requirements will be difficult to understand, apply or resource.

5. Notwithstanding the above, AusCERT fully supports education and awareness raising programs that help account users understand and reduce the risk of malware compromise to their computers. AusCERT does not support 'awareness raising' programs which downplay the nature of the threat and risk and provide simplistic and inadequate advice about the security counter-measures that should be adopted just to make the messages seem more palatable to users. A simplistic approach, by its shortcomings, can leave users with a false sense of security and unable to adequately reduce the risk[3] in the current threat environment.

6. While it is agreed that a "properly secured PC or other [computer]" is indeed required to substantially reduce the risk of malware compromise, the problem is less to do with the presence and use of user-controlled applications and more to do with the design and security of the underlying operating system software. Many information security experts argue that main stream operating systems (MSOS) such as Microsoft Windows, Apple Macintosh and various UNIX proprietary and open source platforms are simply not designed to withstand malware compromise and all can be potentially subverted due to software vulnerabilities in these platforms.[4]

Factors which increase the difficulty that even motivated and IT-security literate users have to protect themselves from malware attack when conducting online banking:

7. In the last 12 months AusCERT has observed a substantial increase in use of near zero-day[5] exploits being used to support malware attacks designed to steal online banking credentials. The use of zero-day and near zero-day exploits mean that a user's computer may still be successfully compromised with

---

[2] See AusCERT's *Protecting your computer from malicious code*, available at http://www.auscert.org.au/3352

[3] The reviewers should be mindful that account users are also vulnerable to the loss of a range of personal information as a result of online attacks – it is not just the potential dollar loss from their bank accounts which is at stake. Therefore, such users have a right to understand the real risks involved in using the online channel with regard to the protection of their personal information.

[4] For further details about this point, please refer to AusCERT's submission to the e-Security National Agenda Review, Section 4.1, http://www.auscert.org.au/download.html?f=224

[5] A zero-day exploit is one that exploits a software vulnerability which was not publicly known until the same day the attack occurred and for which there is obviously no software security patch yet produced and available to prevent the attack. A near zero-day exploit is one that is exploited very soon after the public disclosure of a new software vulnerability but before the software vendor has time to investigate, develop and distribute a patch for the vulnerability.

malware despite their best endeavours to keep operating and application software up to date and following good practice recommendations.

8. Similarly, most new malware variants which target online banking account users have proven to be undetectable by many anti-virus products at the time it is released and discovered by information security professionals which is generally the same time it is attacking potential victims' computers. Therefore, for many users with up to date anti-virus software, their computers will not be protected from compromise by such malware if they were targeted.

9. A large proportion of malware which is designed to target online banking account users which is being developed and released relies on social engineering as the initial mechanism to commence the infection process. Therefore, merely taking steps to reduce the vulnerability of the user account computer/equipment while highly desirable, will not necessarily be sufficient to prevent malware compromise. If the user does not understand that:

   - their actions may result in the installation of malicious software (therefore it occurs without their knowledge or consent in the background – unseen by the user); or

   - the software they are installing with user knowledge and consent could be, or is malicious,

   then the user can potentially override the security of their own computer unwittingly, regardless of the presence of other security counter-measures.

Additional comments in relation to points raised in discussion paper[6]:

- Potential impact on consumer confidence.
  - AusCERT agrees with points raised in paper.
- Potential impact on development of other fraud counter measures.
  - AusCERT agrees that the only effective long term solution to malicious code related fraud is to make the online channel more secure independently of end users *and end users' computers.* Arguably if financial institutions implement mechanisms which provide added security, independent of users and their computers, it may increase user confidence in use of the online channel and further increase financial institutions' cost savings.
- Complexity/cost of administration
  - The proposal to shift liability to account users for both malware related attacks and deceptive phishing attacks would require an expensive and complex mechanism to evaluate if the user is liable under these conditions. To be fair and transparent in any evaluation process, it would be necessary to conduct an expensive and time consuming

[6] Table 9, page 65 refers.

forensic examination of the computer or computers the user used for an unspecified period prior to the fraud occurring. It is likely the cost of the evaluation process would far exceed the cost of any actual loss to an individual user.

- Potential for harsh/unfair outcomes for account holders
    - If liability were to accrue for malware related attacks, it is unclear what the minimum security requirements expected of account users would be. Who would decide what they should be and whether such requirements would be effective in reducing the risk to which users and financial institutions are currently exposed or are likely to be exposed in future?
    - If the onus remains on the financial institution to prove that the account user was liable under these circumstances, the user would presumably be forced to comply with a privacy-intrusive forensic examination of their computer or if they refused, bear the liability for the attack without the institution proving its case that the account user actually contributed to the attack. What would occur if the computer did not belong to the account user, but rather a third party? How would their privacy rights be protected?

Liability for losses resulting from deceptive phishing attacks

Q29

AusCERT would not support any major change to the current liability arrangements of the code to include liability arising from a user responding to a deception-based phishing attack.

10. As noted in the discussion paper, a large proportion of current online ID theft attacks are the result of phishing[7] – a social engineering technique designed to fool users into disclosing banking credentials, such as user name and password. In these cases, no malware is present on the phishing site or required to be installed on the account user's computer for the attack to occur.

11. To shift the liability to users in this situation implies all account users can recognise a fraudulent email and/or web site and that they deliberately choose to disclose their account credentials to a potential attacker and risk funds loss. This is an erroneous assumption on a number of levels:

    a. Firstly, the nature of the attack is such that if the users' were not fooled in the first instance then the user would not have disclosed their account

[7] Some sources (including the EFT Code Discussion paper) refer to phishing attacks as any online attack which steals banking or online access credentials, whether it involves the use of malware or social engineering (deception). However, AusCERT uses the term online ID theft attacks of which phishing and ID theft trojan attacks are two distinct forms. Both types of attacks typically use social engineering as the initial mechanism to fool users taking unsafe behaviour online. However, phishing uses a fake imitation email and/or web site to fool users into disclosing their access credentials. The idea is that users believe they are communicating and connected to their trusted online bank web site when in fact they are communicating with a fake site controlled by an attacker.

credentials in the second instance. Therefore, changing liability will not reduce the level of fraud – it only shifts the losses from the financial institution to the account users who can least afford to bear the loss.

b. Secondly, while some phishing attacks are quite rudimentary, others are more sophisticated and it can be extremely difficult even for cautious, IT literate account users to distinguish a fraudulent site from a legitimate site. There are a variety of techniques[8] used by attackers to enhance the seeming legitimacy of a fraudulent site. Given the sophistication of many of these attacks – it is assessed to be unreasonable to expect that average account users will always be able to discern the difference in all cases. It would be similarly unreasonable to make them liable in such a case.

c. The current code makes it clear that account users should not be held liable for a faulty access code. Yet single factor authentication credentials can be easily captured and re-used and in the vast majority of deception-based phishing attacks and malware attacks it is single factor authentication credentials which are fraudulently captured and re-used. Hence arguably the problem is with the authentication mechanism rather than the account user, in which case liability should not accrue. Strong forms of two-factor authentication would prevent most current forms of phishing attacks.[9]

More effective, alternate risk reduction strategies

12. It is AusCERT's view that there a range of risk mitigation strategies which could be implemented to help reduce the risk of loss to both account users *and* financial institutions due to fraudulent unauthorised transactions by third parties which does not place potentially onerous security requirements onto account users.

13. One relatively simple and currently effective method of preventing fraudulent and unauthorised transfers of funds from user accounts is to use a two factor authentication mechanism which uses a keyed hash function to digitally sign

---

[8] The techniques are numerous but include techniques referred to in the following papers :

Implications of trends and developments in online ID theft, No. 1, available at https://www.auscert.org.au/5768;

Trends and developments in online ID theft – update, no. 2, available at https://www.auscert.org.au/5769;

Managing risk associated with online ID theft for government and providers of e-government services, available at https://www.auscert.org.au/5777;

Haxdoor – an anatomy of an ID theft attack using malware, available at https://www.auscert.org.au/7069.

Many of these techniques involve the clever manipulation of IT technology and some include the use of malware to modify the screen output to increase user deception.

[9] There are some other forms of phishing attack which will not be prevented using some types of two factor authentication but these types of attack are not as commonplace at present. For example, phishing for Transaction Authentication Numbers (TANs). Also refer to the recent ABN AMRO attack raised in footnote 10.

each transaction (such as a funds transfer) that a user performs *and for the keyed hash to be calculated off the untrusted device* (ie the account user's computer). The Europay, Mastercard, Visa (EMV) chip and pin specification has this functionality and the Barclays bank will be adopting this form of authentication in the near future. This form of two-factor authentication differs markedly from most other two-factor authentication mechanisms currently in use in Australia, and indeed, many other parts of the world.[10] [11] The unique advantage of the mechanism is that it has the ability to still protect the integrity of transactions undertaken even in the event that the account user's computer is compromised with ID theft trojan/malware. [12]

14. Similarly, as noted in paragraph 7.25(a) of the discussion paper, if a financial institution determines that some account holders are repeat victims of malware and deception-based phishing attacks – whether due to perceived negligence or user ignorance – and are therefore a higher risk than the majority of account holders, AusCERT supports their prerogative to reduce their risk by denying these small number of account users access to the online channel.

---

[10] Most simple forms of two-factor authentication, including through the use of a hardware token which generate a one time password and challenge-response are vulnerable to malware attack. That is, the trojan, once installed on the account user's computer simply waits for the user to establish a legitimate login session with their bank using their multi-factor credentials. Then the trojan then can conduct funds transfer in the background without the user's authorisation or knowledge. To the financial institution, the funds would appear to have been transferred and authorised by the account user. A slight variant of this example, involving a hybrid phishing and malware attack, reportedly targeted ABN AMRO's online banking customers recently. Details are available at http://www.out-law.com/page-7967

[11] For further information about the EMV specification and the risk to online users refer to the UK Association of Payments and Clearing Services. (www.apacs.org.uk).

[12] The authentication mechanism – like all other authentication mechanism cannot prevent the breach of confidentiality of account user data or information if the account user's computer is already compromised with ID theft malware. However, if the key goal is to ensure only authorised transactions occur from online accounts and thus to reduce the risk of losses to both financial institutions and account users, this mechanism will provide that protection.