THE PRACTICAL SECURITY OF OUT-OF-BAND TRANSACTION VERIFICATION METHODS

Ref: TR 02/10-SN2202
Version: 1.0r1

EISST Ltd

Fairfax House
15 Fulwood Place
London, WC1V 6AY
United Kingdom
T: +44 (0)20 77 483 237
F: +44 (0)20 77 483 273
E: info@eisst.com
W: www.eisst.com

Table of Contents

Prologue

The system 3-D Secure (3DS), known also under the names Verified by Visa and MasterCard SecureCode, has recently undergone severe scrutiny and hard criticism by security experts and the media alike[1]. Implemented and paid for by e-commerce vendors, the system requires users to enter a password or portions of a password to complete an on-line purchase. The security of the current implementation of 3DS is considered insufficient mainly because of the following flaws:

- weak user enrollment process
- lack of mutual authentication between the client and the authentication server
- inability of the users to distinguish the 3DS genuine *iframe* from fraudulent windows

Indeed, it is currently recognized that 3DS exposes online transactions to a host of very powerful, yet simple to deploy, attacks from organized e-criminals. In particular, 3DS is currently prey of massive phishing scams, accounting for over £300 Million bank fraud losses during 2008 in the UK alone.

Despite such vulnerabilities, 3DS is still the most used single-sign-on system in the world, with over 250 Million users of Verified by Visa alone. Such massive deployment has prompted the development of ever more effective phishing scams and, as a consequence, an increased attention from governmental and regulatory authorities in defense of consumers.

In a recent interesting paper, *Murdoch and Anderson* analyze in detail the 3DS process and reach the following conclusion concerning possible fixes:

"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 or CAP (Chip Authentication Program) 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."

---

1. See for example:
- http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf
- http://www.thetechherald.com/article.php/200947/4815/Phishing-Verified-by-Visa-scam-targets-holiday-shoppers

Problem Statement

In the cited publication, *Murdoch and Anderson* advocate the use of an out-of-band trusted communication channel supported by a simple (but desirably tamper-proof) USB device with a trustworthy display (hereinafter we will refer to such a device with the acronym TOOBAD, standing for: Trustworthy Out Of BAnd Device).

The TOOBAD value proposition hinges on the ability to communicate directly to a customer the details of the transaction, bypassing the insecure environment of the PC, and thus providing the required security assurances. A large number of experts and professionals in the security business are likely to agree with this approach, which – as the authors also stress – is not very complicated, can be deployed at a reasonable cost and, most importantly, provides *provable* transaction security.

Notwithstanding the validity of all the above considerations, our analysis (confirmed by results from field observations) suggests that once deployed the TOOBAD may not deliver all the security assurances it seems to promise. In this paper, we wish to briefly address the following very basic questions:

Q1- What should be the primary goal of a successful transaction authentication method?

Q2- What is the key factor ultimately determining the security of an online transaction?

Q3- What will be the result of attacks launched against a transaction validation process based on the TOOBAD?

and, finally:

Q4- Can a transaction validation process based solely on the use of a TOOBAD device prevent the massive fraud losses currently plaguing online financial transactions?

While answering these questions we recognize that the ensuing discussion will not reach the depths of rocket science. We are, nevertheless, hopeful that it may contribute to a better understanding of how TOOBAD devices can help neutralize e-criminal attacks with the level of sophistication currently observed in the wild.

Observations

Most security practitioners would agree that a principal goal of any improved transaction validation method should be a high transaction *efficiency,* i.e. the ability to reduce the current level of exposure to online fraud while at the same time enabling a growing number of legitimate transactions. In the context of this discussion, this implies that any improved methods should be able to raise the hacking efforts required to fraud e-payments and Web transaction systems well above those of phishing scams currently plaguing the online business community. Thus, our suggested answer to the first question is:

A1- It should allow to substantially increase the number of legitimate online transactions.

Please note that our answer doesn't focus on the ability to stop fraudulent transactions, but rather it stresses more the need to support the online business model, whereby end-users should become growingly confident in their ability to successfully and securely carry out sensitive transactions over the Internet. In other words, improving the detection of fraudulent schemes without providing means for increasing efficiency will not serve the end purpose and ultimately frustrate end-users and raise questions on the sustainability of the online business model.

The above considerations place the focus where it is due, i.e. on the end-user. Indeed, it is a very common experience for security professionals to observe sophisticated security measures totally thwarted by careless or silly end-user behavior. Thus, our answer to the second question is:

A2- An end-user behavior supporting and enabling the security measures put in place for protecting the online transaction.

At the risk of restating the obvious, there is nothing one can achieve in security without a collaborative and smart participation from the part of the end-user. The flip side of this statement is evidently somewhat less obvious: security measures which rely on the end-user's judgment call, must also assure protection against attack vectors allowing to steer or influence the same end-user behavior. Indeed, one golden rule in designing good security solutions should be to avoid at all costs having to rely at some point on the end-user ability to make the right decisions. Whenever this cannot be avoided, one should at least put in place equally strong protections in support of all the interface elements which impact the end-user decision making and cognitive abilities during the transaction process. Thus, our answer to the third question is:

A3- An increased level of unsuccessful transactions. Induced end-user confusion leading to unsecure actions (or otherwise unaware behavior) often enabling fraudulent transactions and lowering end-user confidence.

Here we reach the paradoxical (but quite obvious) conclusion that a provably secure system may be shown to be *practically insecure* (whenever it calls for a proper behavior of an ill-influenced end-user) and *practically inefficient* (whenever it allows attackers to easily manipulate the transaction environment, such as the user interface elements). Plenty of examples can be drawn from the security literature in support of this conclusion, whereby hackers are capable of inducing individuals into neutralizing or misusing even very sophisticated protection techniques. The point we wish to make in the context of this paper is more explicitly that the social engineering attack vector is highly potentiated by the interface manipulation attack vector and that such synergy may lead to the practical failure of otherwise theoretically sound security measures. Thus, our answer to the last question is:

A3- Most likely, no.

The above conclusion is supported by a field study carried out using a test e-banking scenario, wherein end-users were asked to complete online transactions in a controlled environment using a standard Web browser and a simulated TOOBAD device. The end-users were instructed to login using a strong authentication method (e.g. fingerprint scan) and then to carefully check the transaction details before authorizing any payments. In particular, the account number of the beneficiary was displayed and showed to the end-user on a separate screen before the authorization step could be completed. The end-users could then authorize or abort the transaction by clicking on two separate buttons (red, not OK – green, OK). During the sessions, the end-users were presented with several real-life legitimate and fraudulent scenarios, including maintenance and support messages from the Bank personnel, phishing scams and more sophisticated attacks using social engineering and interface manipulation vectors (see the Appendix for what turned out to be one very powerful attack scenario inferred from the toolkit of Zeus, one of the most successful and deployed financial malware codes).

Results suggest that the *practical* security of transaction validation methods based solely on a TOOBAD device is only marginally better than the security attainable using less sophisticated (and costly) methods. In particular, the ability to manipulate the user interface of the Web browser during the transaction procedure enabled crafting a number of very effective attack schemes for inducing the end-users into authorizing fraudulent money transfers. Even more significantly, whenever the end-user was alert enough to understand the danger and stop the attack by clicking on the red button, he/she voiced a strong disillusion with respect to the trustworthiness of the overall business process sponsored by the Bank.

The key factors underlying the above observations can be summarized as follows:

- The end-user's acceptance of a new transaction process based on the external device with a high-tech look requires explaining the unique security benefits of such scheme. In order to surmount the acceptance hurdle (sustained by the innate human resistance to change), the end-user is induced (forced) to place uncritical trust in the effectiveness of the new security process (otherwise, why bother?).

- During the online transaction, the main focus of the end-user's experience is captured by the PC interface elements and delivered via the Web browser GUI components. These latter have a stronger influence on directing the end-user decision process with respect to the data displayed on the external device.

- The end-user doesn't critically analyze the Bank's Web site appearance, structure or any interactive messages displayed during the session. Once the user is logged-in and operates within the e-banking environment, he/she believes in the integrity of the Web experience.

Conclusions

The current state of affairs regarding the security of online transactions can be aptly summarized by the following two recent expert statements[2]:

Ross Anderson, Prof. Security Engineering, Computer Labs, University of Cambridge:
"Computer criminals differ from ordinary criminals in that they're more rational. The bulk of street crime is done by disadvantaged young men, often illiterate and with drug or alcohol problems. **The bulk of e-crime is done by technically sophisticated people**… So while preventing normal crime is about sociology, **preventing online crime is about economics**. **Malware writers are rational, as are botnet herders…**. "

Robert G. Ferrell, Information Systems Security Specialist, U.S.A Dept. of Defense:
"….. **Far more relevant to security are the browser clients a consumer is using, irrespective of the operating system or hardware platform**. Even more critical from a safety standpoint is the level of security awareness exhibited by that consumer. If you haphazardly visit every Web link …**sooner or later you're going to get nailed. Period**. **Platforms are passé. Applications are where it's all at**."

When evaluating new technologies for protecting against attacks from e-criminals one must then carefully consider the following questions:

- Will the solution sensibly impact the hacking economics, or – to put in terms of a familiar terminology - will the new protections drastically lower the e-criminals' ROI ?

- Does the solution provide relief against the most exploited vulnerabilities known today to plague e-commerce and e-banking transactions?

The analysis described in the previous sections suggests that the use of trusted out-of-band devices for transaction verification may fall short on both these criteria unless such devices are supported by additional security measures. In particular, it appears essential to extend security beyond the transaction authentication stage to protect also the UI transaction context and in particular the Web Browser, which is widely recognized as the main source of security vulnerabilities exploited by e-criminals today.

---

2. http://news.cnet.com/8301-27080_3-10444561-245.html

Appendix: Example Attack Scenario

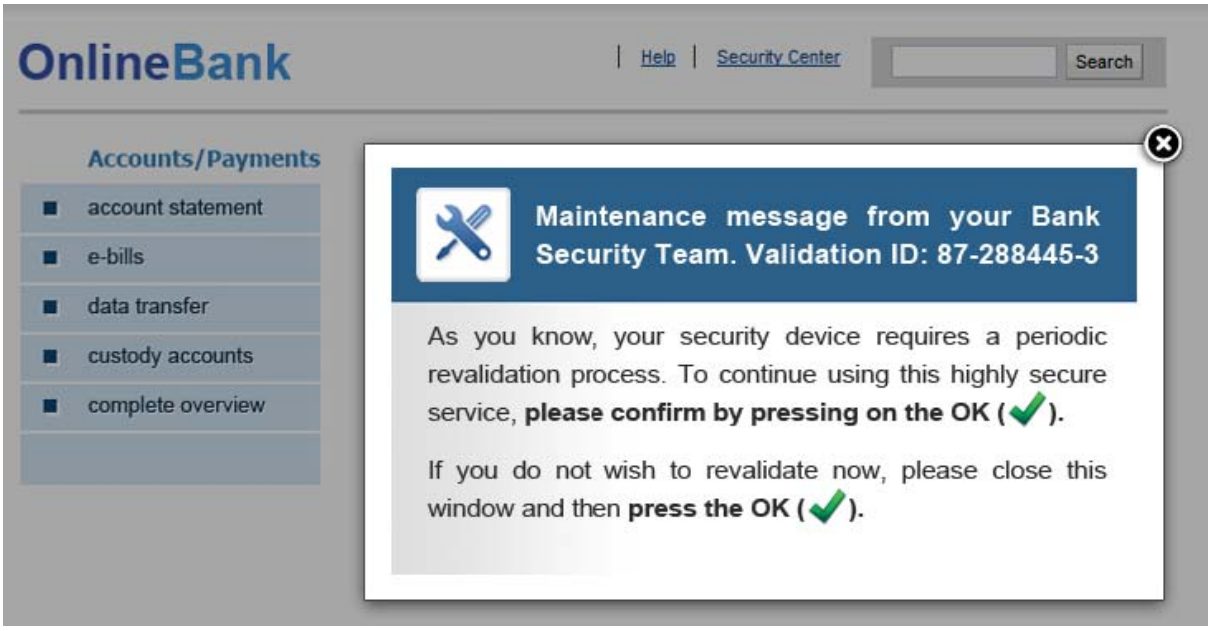
NOTE: This attack scenario can be viewed online at the following link
http://www.h-browser.com/video/toobad/

1. The Hacker deploys malware onto the Victim's PC.

2. The Victim logs in to his/her Bank and starts a session using a standard Web Browser.

3. The Victim now plugs in the PC his connected security device and has access to his e-banking account page.

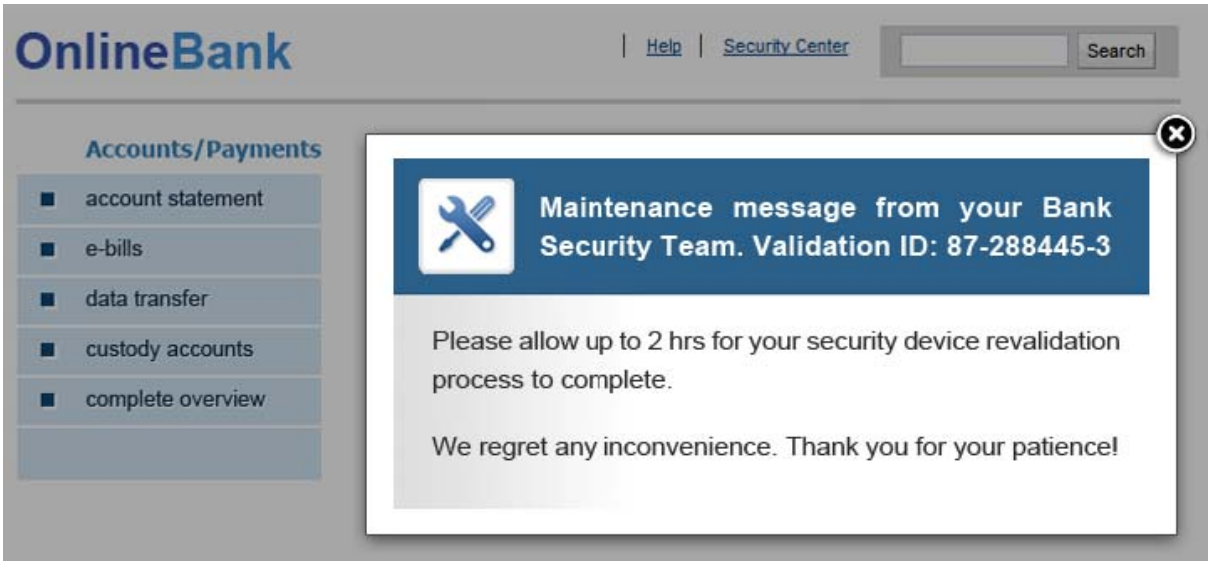
4. The malware is activated and shows a pop-up window with the following message:



5. While showing this message, the malware is actually carrying out in the background a fraudulent transaction of funds to the Hacker's Bank account 87-288445-3.

6. The Victim checks his external security device and sees the code 87-288445-3. Since he wishes to continue using the security device, the Victim clicks on the OK button.

7. The malware now allows the Victim to operate on his account only in a limited way and then closes the connection with the message:



8. The malware then blocks any further access to the Victim's e-banking account from that PC for a period of time to allow the fraudulent transaction to be processed by the Bank.