Source: Marko Hölbl, CEPIS LSI Secretary **Version v2.7 / 24/10/2007**

Document for:

Decision	
Discussion	**X**
Information	

Authentication approaches for online-banking

Background Paper

1 Introduction

Online-banking (i.e. the possibility to initiate financial transaction via an online (Internet)-connection to one's bank or other financial institution) is an appealing way of doing business. The adoption of online-banking of internet users in the EU-25 is currently 36% [ES16]. However in recent years we have witnessed the increase of online-banking abuses. Since online-banking is used widely, malicious and criminal users have become interested in it. Especially organized criminal attempts are on the rise.

Consequently, more sophisticated attacks on online-banking have come up. Most recent trends go towards complex phishing (password fishing) attacks. These types of attacks are not pure technical attacks; they exploit on one hand psychological and sociological properties of users and on the other hand technical flaws and weaknesses.

As online transactions require new authentication methods, banks are trying to introduce new approaches in order to prevent attacks being successful and to increase security. The trend goes towards multiple-factor-authentication (mainly two-factor authentication). In fact most banks employ two-factor authentication yet in different ways. Besides usual username/password (or similar) approaches, additional tokens are applied for authentication in order to make online-banking more secure.

Being the voice of European IT practitioners and experts CEPIS is concerned about the abuse of IT: Its main concern is that the continuous use of a security technology that does not improve security but makes applications harder to use for the customer. For example, the iTAN security measure does not raise the security level – but only bluffs security. On the other hand alternative approaches, which could raise security for users are not employed (or rarely employed). Based on those findings CEPIS strongly recommends not to apply unnecessarily complex or cumbersome security technologies. Instead a cost-benefit-analysis should be applied to security technologies, which would asses how effective the protection is and what are the burdens for all the involved parties, including the bank's customers.

2 Authentication approaches

In recent years most banks offer online-banking to their customers. As banking activities are by nature more sensitive than most other Internet activities, higher security standards are required. To increase security, most banks employ two-factor authentication, which involves two basic factors:

- Something the user **knows** (e.g., password, PIN, pass phrase);
- Something the user **has** (e.g., smart card, other hardware token).

The knowledge of username-passwords or pass phrases is the most commonly used authentication method on the internet. Most banks conduct two-factor authentication one of which being based on the knowledge of a piece of data (something the user knows). The actual implementations may vary, still username-password combination, pass phrases or PIN numbers are the most commonly applied. In order to increase security, most banks employ a second authentication factor – a token that the user possesses. The implementations of the authentication factor can be classified as follows:

- a one-time password approach;
- a certificate based approach;
- a timer based (short) password approach;

- a certificate - smart card based approach.

2.1 The certificate based approach

In case of the certificate based approach a certificate is used as the second authentication factor. Certificates are software tokens that require a PKI (public key infrastructure). They can be stored either on the hard drive or another storage device (e.g. USB stick, smart card). Usually banks employ the combination of a certificate together with username-password, pass phrase or PIN number. Clearly the approach is easy to implement and cheap on the user's and bank's side. The approach is susceptible to man-in-the-middle attacks when used without transmission security (e.g. SSL/TLS). Some Slovenian banks use this approach (e.g. NLB).

2.2 The one-time password approach

Tokens in form of one-time passwords (named TANs, transaction authorization numbers) are very popular in German speaking and Scandinavian countries [DB05], [AP]. The main advantage of one-time passwords is the fact, that they can be used only once and become invalid afterwards. Commonly used implementations include iTAN, eTAN and mTAN. iTANs are distributed on lists, whereas eTANs are generated using special hardware devices [DB05]. The third type of TANs, namely mTANs are generated using mobile phones [DB05]. Figures 1 and 2 depict the way traditional TANs and iTANs work. The mTAN and eTAN approach function in the same way, except that instead of paper lists SMS messages or other media are used.

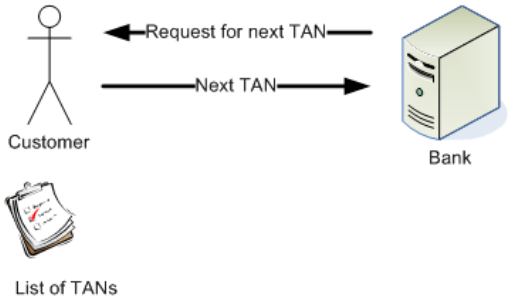

Figure 1: TAN approach

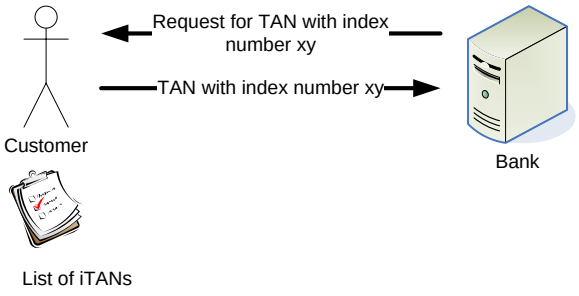

Figure 2: iTAN approach

Recently, the introduction of iTANs (indexTANs) has caused much discussion in the computer security community [CT05], [HB05]. iTANs were presented as being much more secure than their predecessors TANs. TANs are distributed in batches to the customers who later use them sequentially to authorize transactions. Likewise iTANs are distributed in batches to the customers, but customers need to provide one specific TAN from the batch, as is indicated by the banking system. The rationale for the introduction of the iTAN is that an attacker cannot just make use of a stolen TAN, as he cannot control which TAN would be needed. However the iTAN system puts an additional burden on the customer, as he needs to have all iTANs at hand when using the online-banking systems.

It was shown that the system was not as secure as the introducing banks claimed it was (cf. "Usage and Attacks"). Because of recent attacks, banks are considering to replace printed iTANs with eTAN / mTAN generators. Nevertheless, the biggest problem with TANs is the possibility of man-in-the-middle attack. In order to carry out these attacks, the attacker uses phishing techniques to position himself between the user and the bank and presents the user a fraudulent web site of the bank (owned by the attacker) [AP]. Regarding recent reports on the raise of attacks, there are concerns about the security and reasonableness of using TANs.

An approach similar to TANs is used by the Barclays Banks in the UK. A 'PINsentry' device was introduced that is used together with the customer's debit card and a PIN, to authenticate the identity at log-in and for making payments. The approach should replace the need for pass codes and memorable words.

Clearly the approach has some of the properties of TANs. Still, an adversary is able to conduct phishing attacks. Nevertheless, there are no known attacks so far in contrast to the TAN approaches.

2.3 The timer based (short) password approach

The timer based (short) password approach is not only used by banks, but also employed by providers of other services like PayPal or eBay. The timer based one-time-password is generated using hardware generators (e.g. SecurID). Additionally, a PIN or password is used together with the one-time-password. Once the password is generated, it is valid only for a specific time interval (e.g. 60 seconds). However, the approach is not widely used; as we know only the Slovenian bank NKBM uses this approach. The major advantage is that the time for an attacker to carry out attacks is limited. Still the man-in-the-middle attack is possible (if used without transmission channel security – e.g. SSL/TLS), but has to be carried out fast. Furthermore, the approach carries cost on the bank's side and on the user's side.

2.4 The certificate - smart card based approach

Smart cards are known from other fields of computer security. In online-banking they can be used to store certificates or as devices for generating one-time-passwords. When using smart cards, a card reader is essential, which is not a usual feature of a PC. There are various types of card readers. According to the HBCI (home banking communications interface) standard, a card reader of class 2 or 3 [HBCI] is recommended for secure use. Such card readers include their own keypad and processor. When used together with smart card and certificates, it is possible to digitally sign a transaction on the card, so that no data (certificate, PIN) ever leaves the smart card. Attackers which apply Trojan horses are unable to steal a certificate or key log a PIN. Furthermore smart cards are protected by PIN numbers or pass phrases which make it difficult for an attacker to misuse a stolen smart card.
Nevertheless, smart cards are costly and the rarely used for online-banking (e.g. in Germany) despite their benefits. Currently not a single bank makes such an approach mandatory. Most banks delegate the decision, whether to use a certificate together with a smart card (and reader), to the user.

3 Usage and attacks

Clearly there are not many different approaches of two factor authentication in online-banking. In German speaking countries and Scandinavian countries most banks use on of the TAN flavours (iTAN, eTAN, mTAN). Although the banks claim that TANs should prevent attacks there are a lot of published attacks. German scientists have shown that different advanced TAN approaches (iTAN, eTAN) are not more secure than the conventional TAN system and that they are vulnerable to the same type of attacks ([RD05], [Ai05]). The media [CT05], [HB05] is reporting on TAN (in)security. When using certificates without smart cards Trojan horses and key logger attacks are applicable. For the approach using timer based password, only a small number of implementation are known and consequentially not many reports of abuse exist [BLP05], [GI].
Approaches using certificates stored on local hard drives are susceptible to man-in-the-middle attacks, key loggers and Trojan horses. Nevertheless, no larger series of abuses / attacks were reported, as to the small number of banks employing the approach. If the certificates are stored on a smart card, the possibility of abuses by 'Trojan horses' and key loggers is negligible. Some banks are using the latter approach and some German banks intend to switch to smart card in the future.
Approaches using a timer based (short) password approach (e.g. NKBM) are harder to abuse because of their time limit. As for know no abuses were published in media. Nevertheless, possibilities exist, but the probability for abuses is much lower than in cases of TANs.
Irrespective of the authentication approach used, it is advisable to secure the transmission (e.g. using SSL/TLS). In case non-secure transmission is used man-in-the-middle attacks are applicable to most authentication approaches (except the use of certificates and smart cards with readers of class 2 or 3). Irrespective of the security of the transmission and the authentication approach it should be noted that malware (e.g. Trojan horses) can take control of user's computer and initiates unwanted transactions.

4 Concerns

We CEPIS recognize the dangers related to online-banking. In this case our concern as CEPIS is not so much about the imperfectness of security measures because as professionals we are aware that some inefficiencies and imperfectness will always occur. However, we are more concerned about the continuous use of a security technology that does not improve security but makes the application harder to use for the customer. Some security measures, like the discussed iTAN, do not raise the security level – but only give a false impression of security. On the other hand alternative approaches, which could raise security for users are not employed (or rarely employed).
Consequently CEPIS has serious concerns as follows:

1. If organizations require people to use complex and error prone security measures that do not provide any security improvement we perceive this as an unnecessary burden that will discourage or prevent users easily entering the electronic market place. We perceive this as contradictory to European Union goals towards a common electronic market place.
2. Another problem in relation to users is that the persistence use of cumbersome security measures commented on adversely by the media may damage the reputation of all security endeavours. We think in case of bad reputation consumers will lose confidence and trust in security technologies. Such distrust is very damaging as it makes it far more difficult to react effectively to new security threats.
3. Finally, as a professional organization we are concerned of the unprofessional behaviour applied by not fixing known shortcomings. We are worried about the reputation damage to our profession that such behaviour might create in public opinion.

5 Recommendations

Recognizing the importance of on-line access as one of the vehicles for the development of cheaper, faster and more reliable services there are areas of improvement where all involved parties should endeavour to improve towards the deployment of services without unnecessary or excessive risks.
Based on the findings of its highly professional working party CEPIS has developed recommendations to the 4 different parties involved:

1. Banks and other financial institutions and organisations
2. Governments and regulators
3. Professionals
4. Customers.

5.1 Recommendations to banks and other financial institutions and organisations

CEPIS strongly recommends not applying unnecessarily complex or cumbersome security technologies. Instead a cost-benefit-analysis should be applied to security technologies. Parameters should be:

1. Assessments how effective the protection is, especially how much better the system can withstand particular attacks, when the new technology is applied;
2. Assessments of burdens for all the involved parties.

Customers should be informed of risks, existing security measures and of their rights in case of fraud. A bank should inform their customers in an easy to understand manner of their rights and possible help to compensate for their loss in the case of fraud[1]. Customers should also be given a choice of different methods for authentication to be able to select a system that matches their approach to risk.
Financial institutions and organization should inform their customers that the security of their computer is essential for secure online-banking and that security has to be maintained continuously.
In case of fraud the bank should offer all possible assistance to the affected party especially for the reason that normally the possibilities of a bank immensely exceed those of a citizen.
No practitioner should be considered as qualified to work for a bank or to provide services to a bank without being a member of a professional association that has adopted a code of ethics.

[1] Such as e.g. air travellers have in all EU countries' airports.

5.2 Recommendations to governments

Legislation should be in place to protect customers in cases of online-banking frauds (where existing laws are not adequate or sufficient) and compensate for their customers' losses in proportion with the adequacy of the bank security measures.
Users should not be the only ones to carry the burden of the consequences of criminal acts related to online-banking especially if such acts are made easier due to (insufficient) bank security measures.
Customers should be informed of existing security measures and of their rights in case of fraud.

5.3 Recommendations to professionals

We encourage professionals to uncover problems with e.g. unnecessarily burdensome security technologies and work towards fixing such problems.
Professionals should decline their services to banks in certain cases (e.g. intentionally hidden cost of bank transactions, vulnerability of transactions, and unnecessary disclosure of personal data and similar).

5.4 Recommendations to customers

Customers are encouraged to enquire about security measures and bother to read the small print of the related conditions. Furthermore they are encouraged to include the security of their electronic transactions into the consideration which bank to choose, i.e. not simply to go for the cheapest offer or that with the most aggressive marketing campaign. Customers should continuously maintain the security of their computers in order to support secure online-banking.

6 References

Ai05	iTAN nur in Verbindung mit SSL sicher, A-i3 Ruhr Universität Bochum, https://www.ai3.org/images/stories/pressemeldung/pressemeldung_itan_lang.pdf, 2005
AP	Anti-Phishing Working Group, www.antiphishing.org
BLP05	A. Biryukov, J. Lano and B. Preneel, Recent attacks on alleged SecurID and their practical Implications, Computers & Security, Volume 24, Issue 5, August 2005, Pages 364-370
BS05	B. Schneier, Two-Factor Authentication: Too Little, Too Late, Comm. ACM, vol. 48, no. 4, 2005
CT05	iTAN-Verfahren unsicherer als von Banken behauptet, c't Ausgabe 19, 2005, S. 59, Heise Zeitschriftenverlag
DB05	D. Bachfeld, Nepper, Schlepper, Bauernfänger – Risiken beim Online-Banking, c't Ausgabe 22, 2005, Heise Zeitschriftenverlag
ES16	Online banking: What we learn from the differences in Europe, Deutsche Bank Research, EBanking Snapshot 16, February 2006, www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000196129.pdf
FFIEC	Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, www.ffiec.gov/
FL06	F. Lindner, Citibank does not play dice: Non-random TANs weaken online banking security, Heise Security, www.heise-security.co.uk, 2006
GI	GI warnt vor unsicherem Onlinebanking, Gesellschaft für Informatik e.V., www.gi-ev.de/aktuelles/meldungsdetails/meldung/152/
HB05	Neue Sicherheitslücke gefährdet Online-Strategie der Banken, Handelsblatt Nr. 219, p.26
HBCI	Home Banking Computer Interface, www.hbci-zka.de/
HKW05	A. Hiltgen, T. Kramp, W. Weigold, Secure Internet Banking Authentication, IEEE Security & Privacy, vol. 4, no. 2, 2006, IEEE
JB02	J. Birkelbach, Wege zur Bank Zugangskanäle und -sicherung beim Online-Banking, c't Ausgabe 19, 2002, Heise Zeitschriftenverlag
PG06	P. Gabrijelcic, Elektronsko bancnistvo v Sloveniji (Electronic banking in Slovenia), Monitor, Februar 2006
RD05	Advisory: New banking security system iTAN not as secure as claimed, RedTeam RWTH Aachen, www.redteam-pentesting.de/advisories/rt-sa-2005-014.txt (2005)