Man-in-the-Middle Attacks against the chipTAN comfort Online Banking System

RedTeam Pentesting GmbH

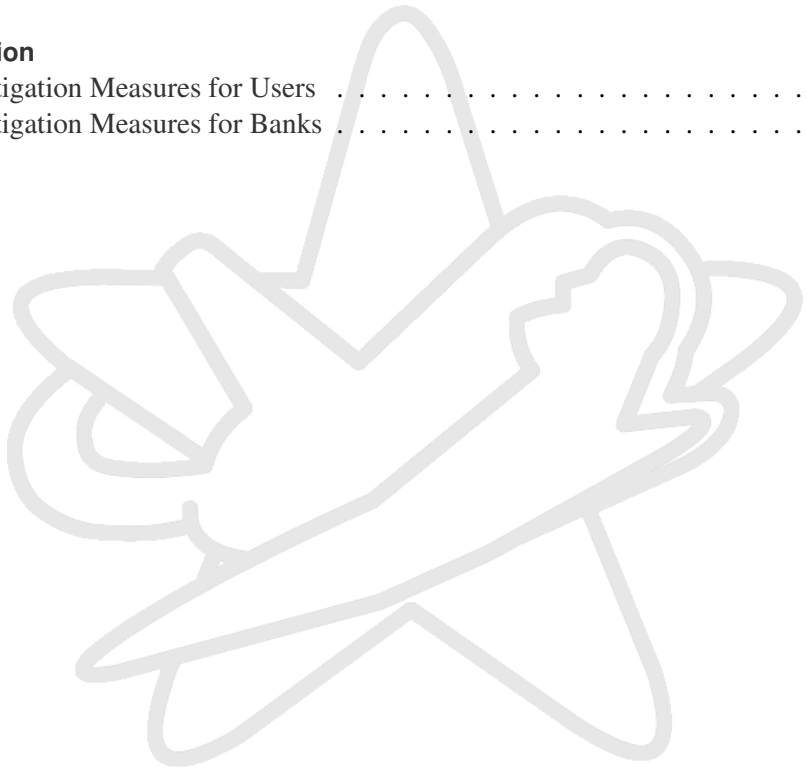
November 23, 2009

http://www.redteam-pentesting.de

ChipTAN comfort is a new system which is supposed to securely authorise online banking transactions by means of a trusted device. It is assumed that chipTAN comfort specifically protects against man-in-the-middle attacks. Such attacks are currently putting bank customers who are using the iTAN system at risk. RedTeam Pentesting examined chipTAN comfort and showed that even when using this system, man-in-the-middle attacks can compromise online banking security.

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

Contents



kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

1 Introduction

Today, online banking is offered by many large banks as an alternative to paying a visit to the bank or to telephone banking. It enables bank customers to do bank transfers or other transactions over the Internet. To protect online banking users against fraud, different systems were developed over time. Currently, most banks in Germany use the PIN/TAN- or the PIN/iTAN system. To further improve online banking security, new systems are currently being introduced, among them chipTAN comfort, which is presently offered to customers of the German *Sparkassen* banks. As there are no publicly known security vulnerabilities in the chipTAN comfort system so far, RedTeam Pentesting examined it for possible attack vectors.

1.1 PIN/TAN System

With the conventional PIN/TAN system, users log into the online banking website with their username and a personal identification number (PIN) and authenticate every transaction with a transaction number (TAN). TANs are normally provided by banks on paper lists and can be used in arbitrary order.

The PIN/TAN system is vulnerable to a range of attacks, among them simple *Phishing*. Here attackers lure users onto a fake online banking website and ask them to provide login credentials and one or several TANs. The collected data can afterwards be used by attackers for their own transactions at an arbitrary time.

1.2 PIN/iTAN System

As a consequence of the Phishing attacks against the TAN system, banks introduced the indexed TAN system (iTAN). In this system, TANs on the (paper) list are numbered. After entering the transaction data, the online banking website prompts the users for a particular TAN (e.g.: TAN No. 23). This TAN is then only valid for the previously entered transaction. This technique is supposed to prevent fraudsters from using intercepted TANs for their own transactions. Binding TANs to specific transactions supposedly renders them worthless for attackers.

In 2005, RedTeam Pentesting showed[1] that these systems are also vulnerable. By performing a so-called *man-in-the-middle attack*, it is possible to request an iTAN for an attacker-provided transaction instead of a user-provided transaction. Since 2008 at the latest, the attacks presented

[1] `http://www.redteam-pentesting.de/advisories/rt-sa-2005-014`

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

three years before are being actively exploited, harming bank customers (cf. Bundeskriminalamt: „Kernaussagen zur IuK-Kriminalität 2008“[2]).

During a man-in-the-middle attack, attackers control the data communication between users and the online banking website. They can therefore read and manipulate all data flowing in both directions. To achieve this, several possibilities exist. Most of the time, the users' computers get infected by malware (e.g. a "Trojan") and all data communication is redirected over an attacker-controlled system. Such a program can also manipulate users' browsers in a way that allows attackers to completely control all content that is displayed.

Afterwards, attackers can detect transactions being entered by users and substitute them with their own transaction data. Any iTAN requested by the bank is in consequence bound to the attackers' transaction and not to the users'. As attackers can arbitrarily manipulate all information displayed by the browser, this attack is not recognisable for the user.

1.3 chipTAN comfort System

The chipTAN comfort system is presently offered by many Sparkasse banks as a further development of the iTAN system. It focuses on the usage of *two factor authentication* by adding a separate, trusted device to the online banking process.

Instead of a TAN or iTAN list, bank customers (in the following: users) receive a device from their bank that has the dimensions of a pocket calculator and features its own display and keyboard. There is also a slot for the banking card as well as five optical sensors on the back side of the device.

Users still enter their transaction data on the computer, for example at the bank's online banking portal. Afterwards, the bank generates a so-called *flicker code*. It consists of five vertical bars switching their colour from black to white in a certain pattern. For simple bank transfers, for example, the flicker code contains the amount of money and the recipient's bank account number. Users place the device in front of their screens and data gets transferred contact-free to the device, using the optical sensors and the flicker code. Afterwards, users have to verify the amount of money and the account number that is displayed. The device will then generate a TAN number only valid for this transaction. The TAN then has to be entered at the online banking website, to authorise the transaction with the bank.

If users' computers are compromised, attackers can manipulate the transaction data if users are utilising the TAN or iTAN system. With the chipTAN comfort system, some of the transaction data is also shown on the display of the trusted device, so that users can detect manipulations. Attackers would have to manipulate the transaction data with a man-in-the-middle attack and

[2] http://www.bka.de/lageberichte/iuk/2008/kernaussagen_iuk_2008.pdf

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

also change the data displayed on the device. As this assumes physical access to the device, such an attack is deemed unlikely.

2 Man-in-the-middle attacks against chipTAN comfort

The iTAN system is vulnerable to man-in-the-middle attacks. As mentioned in the introduction, such attacks are taking place since 2008 at the latest. As chipTAN comfort is an advancement over iTAN, it is supposed to ensure an improved security level, particularly against man-in-the-middle attacks.

In the following, the security of the chipTAN comfort system will be examined in such a situation. The assumption is made that the users' computers are infected with a specialised malware ("Trojan"), which is able to read and manipulate all data communications.

The examination at hand of the chipTAN comfort system is not exhaustive. In contrast to the iTAN system, chipTAN comfort is supposed to also protect against man-in-the-middle attacks. Therefore, this test concentrates on this vulnerability class.

All attacks presented can be fully automated and do not need any interaction from the attackers. RedTeam Pentesting has developed corresponding proof-of-concept code.

2.1 Collective Transfers

With a collective transfer (German: Sammelüberweisung), users can combine several different bank transfers into one transaction. This transaction is then authorised with only a single TAN. If such a collective transfer is authorised with the chipTAN comfort system, two pieces of information are displayed to users on the trusted device. These have to be approved individually, to prevent man-in-the-middle attacks:

- Total amount of money for the collective transfer
- Number of items in the collective transfer

This method does not provide adequate protection against man-in-the-middle attacks. Attackers can redirect the total amount to a bank account of their choosing, without making the users suspicious. To this end, they can manipulate the data of the individual bank transfers and substitute it with their own bank account data. Only the amount of money transferred should not be changed, so that the total amount does not differ from the total amount of the real transaction. The flicker code shown afterwards is then valid for the attackers' bank transfers. The

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

users do not have the possibility to detect this attack, as total amount and number of items are unchanged.

2.2 Bank Transfers

To authorise regular bank transfers with chipTAN comfort, users have to confirm two items on the chipTAN comfort device's display:

- Amount of money for the bank transfer
- Recipient's bank account number

A corresponding text, telling the users to check these items, is printed on the online banking website along with the flicker code. As both items are shown on the trusted chipTAN comfort device, especially the recipient's bank account number cannot be directly manipulated by attackers without raising the users' suspicion. To still be able to execute a successful attack, attackers can resort to a collective transfer. While users are performing a regular bank transfer, attackers can simultaneously create a new collective transfer. This collective transfer only contains one bank transfer to the attackers' bank account, for the same amount as the intended bank transfer. The flicker code resulting from the collective transfer is then presented to the users instead of the flicker code belonging to the intended transaction. Additionally, attackers can adapt the online banking website's text, so that users are asked to check the amount of money to be transferred and the number of bank transfers to be done.

The trusted display of the chipTAN comfort device now also shows the amount of money and number of bank transfer items, as the flicker code belongs to a collective transfer. This is unknown to the users. The output of the device is therefore consistent with the text of the online banking website. Even users knowing that normally the bank account number and not the number of transfer items is shown will have a difficult time detecting such an attack.

2.3 SEPA Transfers

The target account of a SEPA transfer is given in IBAN notation. IBANs can reach a length of up to 34 characters[3]. To authorise such a transfer, users have to confirm the following data transferred via flicker code to the chipTAN comfort device:

- Amount of money

[3] http://en.wikipedia.org/wiki/IBAN

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

- Character 3 and 4 and the last four characters of the target account's IBAN

Again, there is a text on the online banking website containing the flicker code that details what data to check. If attackers manipulate the bank account data and therefore also the IBAN of the target account, the six characters that will be shown on the display of the chipTAN comfort device will belong to the attackers' IBAN and have to be verified by the users.

At this point however, it is possible for attackers to manipulate the contents of the online banking website. This includes the instructions on how to verify the IBAN. Because of the length of an IBAN, it is likely that the original one contains the digits of the attacker-provided IBAN shown on the display. Attackers can therefore change the verification instructions so that apparently the original, user-entered IBAN is verified, by asking for the corresponding positions in the original IBAN.

If users then enter the TAN generated by the device, attackers can authorise the manipulated bank transfer to the bank.

3 Conclusion

The chipTAN comfort system is vulnerable to the man-in-the-middle attacks presented in this paper. As none of the attacks allow for changing the amount of money unnoticed, chipTAN comfort is still to be preferred over the iTAN system. Additionally, chipTAN comfort is not widely deployed at the moment, so that real-world attacks are currently deemed unlikely. However, the probability of seeing real world exploitation against chipTAN comfort gets higher when more users adopt this new system, similarly to the iTAN system.

Therefore, man-in-the-middle attacks also put bank customers that use chipTAN comfort at risk. The main difference is that, in contrast to the current attacks against iTAN, the amount of money cannot be changed unnoticed.

3.1 Mitigation Measures for Users

To protect themselves against attacks, users of chipTAN comfort should always ensure that they communicate with the real bank and are not victims of a man-in-the-middle attack. Especially the PC used for online banking has to stay free of malware. In practice, this is a very difficult task for most users. However, if man-in-the-middle attacks are avoided successfully, the iTAN system is already considered to be adequately secure.

When performing a collective transfer in connection with chipTAN comfort and a man-in-the-middle attack is conducted in parallel, the attack described in section 2.1 is not recognisable

kontakt@redteam-pentesting.de
http://www.redteam-pentesting.de
Tel.: +49 241 963-1300, Fax: -1304

users.

The presented attacks against classic bank transfers and SEPA transfers can theoretically be recognised by advanced users. The trusted display of the device and the content of the online banking website are coherent, but it could be noticed that the output had a different form in the past.

3.2 Mitigation Measures for Banks

The first measure should be to inform users how exactly the chipTAN comfort device's output should look for each different transaction mode. This would enable advanced users to at least recognise and prevent two of the three attacks. The attack against collective transfers cannot be recognised this way. In the long run, the chipTAN comfort's device display should show all information about the transactions to be authorised, if possible. This would enable users to detect all the described attacks and prevent them.