# Security flaw of iTAN based online banking

Alexander Dörsam
Alois Schütte

a.doersam@gmx.net
alois.schuette@h-da.de

University of Applied Computer Science Darmstadt

## Abstract

This article deals with a risk analysis of transaction number (TAN)-based mechanisms to authenticate the online banking area. The motiviation for this development is to be justified by the ever-growing number of users of online banking. Due to the always increasing number of users, security has become a very important factor. The most serious error in relation to such problems is the danger of underestimating attacks. This paper aims to raise user awareness and the administrators involved. It looks to phishing sites and the various phishing mechanisms. After presenting different concepts, this article will go into depth with one particular concept: the principle of parameter manipulation. The third chapter follows a network attack, which is tuned to phishing. This network attack deals specifically with the sabotage of public networks. It is shown how phishing, in combination with such a network attack, increases in efficiency. The article concludes with a summary and reflection of lessons learned.

**Security flaw of iTAN based online banking**

# 1 Indexed TAN (iTAN)

If a user of an online banking portal accesses his account, he must prove his identity. There are several approaches to authenticate the user. The basic approach is a combination of a username and password to login. To improve security further, authentication is required. In most cases the second identity confirmation is required, to complete a transaction. In this chapter the functionality of the iTAN method is presented, especialy how this process can be attacked. For this process the attacker will already have the victims username and password. In contrast to the TAN procedure, the iTAN process requires a specific transaction number. The iTAN-Model indexes every single TAN with a number. When the user wants to perform a transaction he is asked for a, randomly chosen TAN which would make a “sniffed” iTAN nearly useless because an attacker can not predict which iTAN the online banking portal will be asking for in the near future. Surely the online banking portal needs a limiter to avoid the attacker from making aborted transactions until he is asked for the iTAN number he possesses. Typically the bank will lock the victims account after this is done a number of times. The bottom line is that its not enough to just capture a iTAN, an attacker has to attain an iTAN for his fake transaction. This is the reason for the existence of extensive phishing websites. Such a phishing website claims to be the original online banking portal and asks for the username and password. After the attacking website received the login credentials it starts a money transfer. For this transfer the phishing site needs a valid iTAN. The next step of the attack is to ask the user for this specific and valid iTAN for which the programmers of those phishing websites have different methods. Mostly they send messages and claim the portal needs this iTAN to perform any “necessary” task. The techniques to gather those valid iTAN's is one of the most important parts of attacking. The next chapters will describe these methodes more detailed.

# 2 Phishing Site

Phishing sites are replicas of the original web pages. The goal of these phishing sites are to obtain personal information from users.The basic principle of such a phishing site is to deceive the user. The concept of a phishing site for iTAN can be based on several approaches. One effecitve way is based on parameter manipulation. The above described method, where the attacker asks the user for an iTAN breaks the habit he is used to, which makes it conspicious. The attacker should not try to attain the iTAN by force after the transfer initiation. Compared to the forced iTAN theft, the parameter manipulation subtly gains the users iTAN. The attacker just changes the destination of the transfered money. With this technique, nothing changes to the normal money transaction and the user raises no suspicion. For this method to work, a person must want to make a transaction. Although it is more time consuming, but this method is far more efficient than its predecessor. The described procedure is shown at Figure 1.

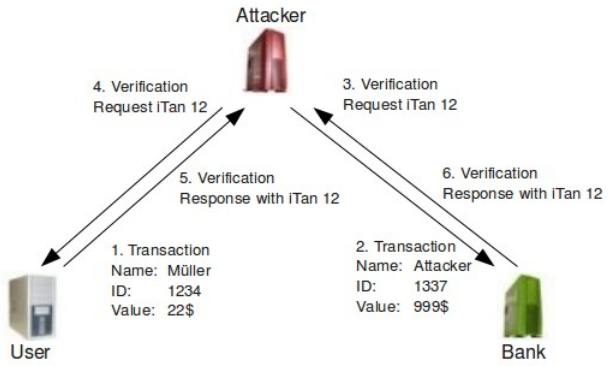


**Figure 1:**

The technical realization of this phishing site was carried out with the programming language "PHP ". If an attacker attempts to create a phishing site, which operates on the concept of parameter manipulation, he must gather information from the online banking system, which is to be attacked. The first step is to identify the Internet address of the online banking system. The example of

## Security flaw of iTAN based online banking

Volksbank would lead an attacker on the home page (http://www.volksbank-xxx.de). There he would look for the link to the online banking page . For example, the target of the online banking link is: https://finanzportal.fiducia.de/ebpp0XX/entryrzid=XC&rzbk=XXX". From this deep link, the attacker first extracts the address of the online banking site: https://finanzportal. fiducia.de. The next step is extract the parameters of interest. For this he starts a transfer and analysis of the source code. This step requires a testing account. The following lines shows the interesting part of the websites source code:

```
<form action="/ebppXX/portal?token=XXXXX" method="XXX">
...
id="txtKontonummerEmpfaenger"
id="txtBankleitzahl"
id="txtEmpfaengerdaten"
...
</form>
```

The marked elements are the parameters which carry the account details. Those parameters are the target of the attacker. Next, an attacker can develop a source code which duplicates an online banking portal and substitude every context of the above shown parameters with his own:

```
<?php
(…)
$callURL = $_SERVER['REQUEST_URI'];
(…)
foreach(explode("&", $callURL) as $key => $val) {
if(preg_match('/txtKontonummerEmpfaenger/', $val)) {
        $val = preg_replace('/=.*$/', '=987654321', $val); }
if(preg_match('/txtBankleitzahl/', $val)) {
        $val = preg_replace('/=.*$/', '=123456789', $val); }
if(preg_match('/txtEmpfaengerdaten/', $val)) {
        $val = preg_replace('/=.*$/', '=Alexander Dörsam', $val);}
        $newURL .= ($key > 0 ? '&' : '') . $val;  }
        $newURL .= ($key > 0 ? '&' : '') . $val;  }
$callURL = $newURL;
(…)
curl_close($ch);
(…)
?>
```

The highlighted elements are the key points of the source code. Those parts replace the content of the identified variables with our own. If an attacker could spread such a website, every transfer would reach the wrong receiver.

# 3 Network Attack

To publish the previously described phishing site, attackers often use fake emails. This paper takes a different way of publishing phishing sites. One of the problems in the dissemination of such replicas is the ratio between the target users and those who actually access the phishing site. A part of this paper is a way to optimize this ratio. The solution of this optimization was sought on public networks. It is a way to manipulate the Internet traffic on public networks so the users are redirected without their knowledge to the phishing site. Such redirecting attacks can be based on the Domain Name Server (DNS) protocol wich is explained as followed: hostnames like “www.volksbank.de” are only a facade. Behind this, the computer talks with such called IP-addresses. Its name exists because its easier for a human to deal with a name than a 32-bit number. To get the association between hostname and IP, a DNS-server is needed. If a user enters “www.volksbank.de” on a browser, his computer asks a DNS-server for the IP-address. Based on the reply of this server, the computer starts interacting with the replyed IP-address. If an attacker could reply with his own, or any of him controlled IP-addresses, the victim will unknowinlgy interact with the server of an attacker when he visits the online banking portal. So the targert of an attacker is to poison this set of hostname and IP-address. The experienced attacker will not try to attack the DNS-servers due to the fact that inside a public network there are weaker targets.
Public networks are defined by agile users joining and leaving its infrastructure. Therefore it is fundamental to serve those volatile clients with the needed network settings. Normaly an attacker finds a so called Dynamic Host Configuration Protocol (DHCP) Server which can do this. In public networks clients have to know which DNS-server they have to ask for IP-addresses. This information is part of the network settings provided by the DHCP-server. So if an attacker could manipulate the DHCP-server, he can manipulate the spread of the reliable DNS-server. In Detail an attacker could reply with a manipulated DHCP-response which includes his own IP-address as a valid DNS-server. This would cause every client to ask the attacker for IP-addresses. In this situation an attacker could answer with his own IP-address if any client asks for an online banking portal. This raises the next question of how to “spoof” the network setting of a DHCP-server. Clarified must be that the DHCP

is capable of more than one DHCP-server on a network. It is possible that an attacker himself offers a DHCP-server in any network, and provides a network configuration. If the attacker operates parallel to the real DHCP-server it is not guaranteed that the user will accept the configurations of the rouge DHCP-server. It is important to find a way corresponding to the user to get them to accept the configurations of the rouge one. So the next Challenge is stopping the real service. In order to achieve a silenced DHCP-server, there is the method of "pool-starving". A DHCP-server has only a limited range of configurations available, a so called pool. This limitation is the result of a network structure which may only allow certain IP-ranges. It could for example be a necessity for only 30 different IP-addresses and therefore 30 different configurations to provide. The concept of "pool-starving" is used to have a DHCP-server which stops after all its configurations are in use. This means that in the case of 30 configurations an attacker may claim to need all of them, which would mute the server. Because there is no strong authentication of users, it is easy to claim 30 different clients and request all configurations a server provides. The only way to authenticate a user is by checking his MAC-address. A MAC-address is theoretically unique and the DHCP-server gives every single MAC-address a set of network configurations. But keep in mind that a MAC-address can be changed easily to any value. An attacker just has to change the MAC-address of a device randomly and request configuration from the DHCP-server to silent it. If the attacker silenced the server he could inject his own machine as a DHCP-server and spread a rouge DNS-Server to the clients.

# 4 Conclusion

The case study confirmed the feasibility of compromising the iTAN process. A demonstration at the University of applied Science in Darmstadt is available, which implements the method described above. The effectiveness of such a system should not be underestimated, because it is able to fool the user almost completely. Surely at present there are alot of techniques to prevent such an attack. The most effective methods are EV-Certificates, which have become standard in context of online banking. Also most of the actual browsers mark online banking portals green when they are trustworthy and it becomes harder to deceive potential victims. This security feature is useless in some browsers such as google chrome. This is due to the hiding of the url in regard to user useability. There are still a large number of services where EV-Certificates are not the norm and therefore prone to phishing. So for users it is a great threat which needs attention of the higher courts. At present the awareness of administrative personal must increase. We noticed during this research that the administrative personal, also in context of high security environments are not as aware as they should be. The analysed banks and companies in context of the research had no interest in working together to make a safer environment. In conclusion, it is not advisable for users to make any sensitive transactions in public networks.
Companies, banks and federal environments transfer far too many important information which makes IT-security not only a fashionable accessory, but a must.

# 5 References

Paul Albitz, Cricket L.: *DNS and BIND. 3. O'REILLY*, 1998. ISBN 1-56592-512-2

Simson Garfinkel, Gene S.: *Practical UNIX & Internet Security*. *2.O'REILLY*, 1996. ISBN 1-56592-148-8

Aurand, Andreas: *LAN-Sicherheit. 1. dpunkt.verlag*, 2005. ISBN 3–89864–297–6

Heise.de: *Verbessertes iTAN-Verfahren soll vor Manipulationen durch Trojaner schützen.* http://www.heise.de/newsticker/meldung/98025

Alexander Dörsam: *Risiko-Analyse von TAN-gestützten Mechanismen zur Authentifizierung im Online-Banking-Bereich, 2008*

Hunt, Craig: *TCP/IP Network Administration. 2. O'REILLY*, 1997. ISBN 1-56592-322-7

Enno Rey: *Netzwerk-Segmentierung und -Sicherheit*. http://www.ernw.de/content/e7/e181/e481/download482/ERNW_Netzwerksicherheit_und_vlans_ger.pdf

APWG: Crimeware and Phishing. *http://www.antiphishing.org/crimeware.html*

*APWG: Phishing Activity Trends. http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf*