Man-in-the-Middle-Angriffe auf das chipTAN comfort-Verfahren im Online-Banking

RedTeam Pentesting GmbH

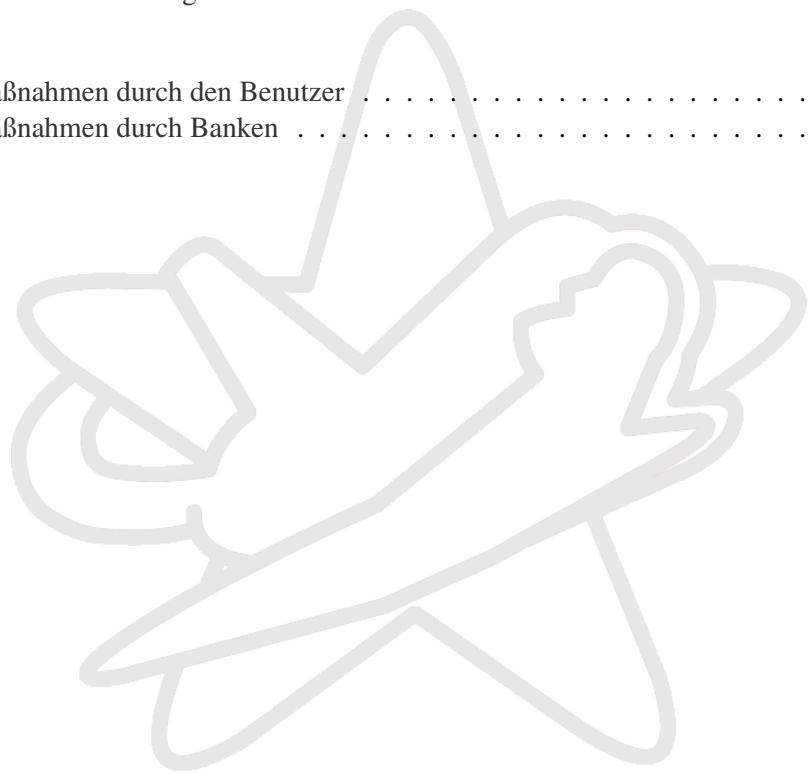
23. November 2009

http://www.redteam-pentesting.de

ChipTAN comfort ist ein neues Verfahren, welches mit Hilfe eines vertrauenswürdigen Geräts Transaktionen im Online-Banking sicher autorisieren soll. Es soll speziell auch gegen Man-in-the-Middle-Angriffe schützen. In der Praxis gefährden solche Angriffe aktuell Bankkunden, welche das iTAN-Verfahren nutzen. RedTeam Pentesting hat das chipTAN comfort-Verfahren untersucht und konnte zeigen, dass auch beim Einsatz dieses Verfahrens Man-in-the-Middle-Angriffe die Sicherheit des Online-Bankings gefährden.

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

Inhaltsverzeichnis



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

1 Einleitung

Durch die große Verbreitung von Internetanschlüssen wird Online-Banking mittlerweile von allen großen Banken als Alternative zum klassischen Besuch in der Filiale oder Telefonbanking angeboten. Bankkunden können so über das Internet Überweisungen und sonstige Transaktionen tätigen. Um die Benutzer von Online-Banking vor Betrügern zu schützen, wurden im Laufe der Zeit verschiedene Verfahren entwickelt. Zur Zeit verwenden die meisten Banken das PIN/TAN- sowie das iTAN-Verfahren. Um die Sicherheit weiter zu erhöhen werden jedoch aktuell auch neue Verfahren eingeführt, darunter auch chipTAN comfort. Dieses wird zur Zeit insbesondere den Kunden der Sparkassen angeboten. Da bei dem chipTAN comfort-Verfahren bisher keine Schwachstellen bekannt sind, hat RedTeam Pentesting untersucht, inwieweit hier Angriffe möglich sind.

1.1 PIN/TAN-Verfahren

Beim klassischen PIN/TAN-Verfahren melden sich die Benutzer mit einem Anmeldenamen und einer persönlichen Identifikationsnummer (PIN) am Online-Banking an und bestätigen jede getätigte Transaktion mit einer Transaktionsnummer (TAN). TANs werden von der Bank in der Regel als ausgedruckte Liste zur Verfügung gestellt und können in beliebiger Reihenfolge von den Benutzern verwendet werden.

Das PIN/TAN-Verfahren ist anfällig für eine Reihe von Angriffen, darunter einfaches *Phishing*. Hier werden die Benutzer zum Beispiel mittels E-Mail-Nachrichten, die vorgeblich von der eigenen Bank stammen, dazu aufgefordert, ihre Anmeldedaten und eine oder mehrere TANs auf einer gefälschten Online-Banking-Webseite einzugeben. Die so gesammelten Daten können anschließend von Angreifern zu einem beliebigen Zeitpunkt für eigene Transaktionen genutzt werden.

1.2 PIN/iTAN-Verfahren

Als Konsequenz aus den Phishing-Angriffen gegen das TAN-Verfahren wurde von den Banken das indizierte TAN-Verfahren (iTAN) eingeführt. Bei diesem Verfahren wird die Liste der TANs durchnummeriert. Nach Eingabe der Transaktionsdaten fordert die Online-Banking-Webseite die Eingabe einer bestimmten TAN (etwa: TAN Nr. 23). Diese TAN ist dann nur für die vorher eingegebene Transaktion gültig. So soll verhindert werden, dass von Betrügern abgefangene TANs für eigene Transaktionen genutzt werden. Durch die Bindung an die Transaktion des Benutzers ist die TAN für Angreifer wertlos.

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

Im Jahre 2005 zeigte RedTeam Pentesting[1], dass auch dieses Verfahren angegriffen werden kann. Durch einen sogenannten *Man-in-the-Middle*-Angriff ist es möglich, die von der Bank erfragte iTAN an eine Transaktion des Angreifers statt des Benutzers zu binden. Spätestens seit 2008 werden die drei Jahre zuvor erstmalig vorgestellten Angriffe auch in der Praxis aktiv ausgenutzt, um Bankkunden zu schädigen (vergleiche Bundeskriminalamt: „Kernaussagen zur IuK-Kriminalität 2008“[2]).

Bei einem Man-in-the-Middle-Angriff („Mann in der Mitte“) kontrolliert ein Angreifer den Datenverkehr zwischen dem Benutzer und der Online-Banking-Webseite. Er sitzt somit „in der Mitte“ zwischen Benutzer und Online-Banking und kann die Datenströme in beide Richtungen lesen und manipulieren. Um dies zu erreichen gibt es mehrere Möglichkeiten. Im häufigsten Fall wird der Rechner des Benutzers mit einem Schadprogramm (Malware, „Trojaner“) infiziert und sämtlicher Datenverkehr über einen vom Angreifer kontrollierten Rechner umgeleitet. Ein solches Programm kann auch den verwendeten Browser so manipulieren, dass die dargestellten Inhalte vollständig durch den Angreifer kontrolliert werden können.

Anschließend ist der Angreifer in der Lage, die von dem Benutzer eingegebenen Transaktionsdaten im Datenverkehr zu erkennen und durch eigene Transaktionsdaten auszutauschen. Die von der Bank erfragte iTAN ist somit für die Transaktion des Angreifers und nicht mehr für die Transaktion des Benutzers gültig. Da der Angreifer die angezeigte Online-Banking-Webseite beliebig manipulieren kann, ist dieser Angriff für den Benutzer nicht erkennbar.

1.3 chipTAN comfort-Verfahren

Das chipTAN comfort-Verfahren wird zur Zeit von einer Vielzahl von Sparkassen als Weiterentwicklung des iTAN-Verfahrens eingesetzt. Das Verfahren setzt auf eine *Zwei-Faktor-Authentifizierung* durch den Einsatz eines separaten, als vertrauenswürdig geltenden Geräts.

Der Bankkunde (im Folgenden: Benutzer) erhält von seiner Bank statt einer TAN- oder iTAN-Liste ein Gerät in der Größe eines Taschenrechners, welches ein eigenes Display und eine Tastatur besitzt. Außerdem sind ein Einschub für die Bankkarte sowie fünf optische Sensoren auf der Rückseite des Geräts vorhanden.

Der Benutzer gibt seine Transaktionsdaten weiterhin über seinen Rechner, zum Beispiel im Online-Banking-Portal der Bank ein. Anschließend wird von der Bank ein sogenannter *Flickercode* generiert. Dieser besteht aus fünf Balken, welche die Farbe in bestimmten Mustern von schwarz auf weiß wechseln. Der Flickercode enthält zum Beispiel bei einer einfachen Überweisung den vom Benutzer eingegebenen Betrag sowie die Kontonummer des Empfängers. Der Benutzer plaziert das Gerät vor dem Bildschirm, so dass über die optischen Sensoren eine berührungslose Datenübertragung auf das Gerät erfolgt. Anschließend muss der Benutzer

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

die auf dem Display des Geräts angezeigte Kontonummer und den Betrag bestätigen, woraufhin das Gerät eine nur für diese Transaktion gültige TAN generiert. Diese muss der Benutzer wiederum im Online-Banking eingeben, was diese Transaktion gegenüber der Bank bestätigt.

Ist der Rechner eines Benutzers kompromittiert, kann ein Angreifer beim iTAN-Verfahren Transaktionsdaten manipulieren. Beim chipTAN comfort-Verfahren werden diese Daten auf dem Display des vertrauenswürdigen Geräts angezeigt, so dass ein Benutzer Manipulationen erkennen kann. Angreifer müssten sowohl mit einem Man-in-the-Middle-Angriff den Datenverkehr manipulieren, als auch die vom Gerät angezeigten Daten verändern. Ein solcher Angriff gilt als unwahrscheinlich, da dies einen direkten physischen Zugriff auf das Gerät vorausgesetzt.

2 Man-in-the-Middle-Angriffe auf das chipTAN comfort-Verfahren

Das iTAN-Verfahren ist anfällig für einen Man-in-the-Middle-Angriff. Wie in der Einleitung erwähnt finden solche Angriffe spätestens seit 2008 statt. Da das chipTAN comfort-Verfahren eine Weiterentwicklung des iTAN-Verfahrens ist, sollte es insbesondere bei Man-in-the-Middle-Angriffen ein höheres Sicherheitsniveau gewährleisten.

Im Folgenden wird die Sicherheit des chipTAN comfort-Verfahrens in einer solchen Situation betrachtet. Es wird davon ausgegangen, dass der Rechner des Benutzers mit einer spezialisierten Schadsoftware („Trojaner“) infiziert ist, welche den gesamten Datenverkehr mitlesen und manipulieren kann.

Die vorliegende Betrachtung der Sicherheit des chipTAN comfort-Verfahrens ist dabei nicht abschließend. Im Gegensatz zum iTAN-Verfahren soll chipTAN comfort auch gegen Man-in-the-Middle-Angriffe schützen. Daher konzentrierte sich der Test auf diese Schwachstellenklasse.

Alle im weiteren Verlauf vorgestellten Angriffe sind vollständig automatisierbar und bedürfen keiner Interaktion durch den Angreifer. Entsprechender Beispielcode (Proof of Concept) wurde von RedTeam Pentesting entwickelt.

2.1 Sammelüberweisung

Mit einer Sammelüberweisung hat ein Benutzer die Möglichkeit, verschiedene Überweisungen zu einer Transaktion zusammenzufassen. Diese wird anschließend mit nur einer TAN bestätigt. Wird eine solche Sammelüberweisung mittels des chipTAN comfort-Verfahrens autorisiert, so erhält der Benutzer insgesamt zwei Ausgaben auf dem Display des chipTAN comfort-

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

Geräts. Diese müssen einzeln bestätigt werden, um Man-in-the-Middle-Angriffen vorzubeugen:

- Gesamtbetrag der Sammelüberweisung
- Anzahl der Posten in der Sammelüberweisung

Dieses Verfahren schützt nicht ausreichend vor Man-in-the-Middle-Angriffen. Ein Angreifer kann den Gesamtbetrag auf ein Konto seiner Wahl umleiten, ohne dass dies für den Benutzer auffällig wäre. Hierzu manipuliert er die Kontodaten der einzelnen Überweisungen und trägt seine eigenen Daten ein. Lediglich die Beträge dürfen nicht manipuliert werden, damit der auf dem Gerät angezeigte Gesamtbetrag sich nicht ändert. Der anschließend angezeigte Flickercode ist somit für die Überweisungen des Angreifers gültig. Der Benutzer hat keine Möglichkeit, diesen Angriff zu erkennen, da die Anzahl der Posten und der Gesamtbetrag unverändert sind.

2.2 Überweisungen

Um Überweisungen mittels des chipTAN comfort-Verfahrens zu autorisieren, muss der Benutzer zwei Ausgaben auf dem Display des chipTAN comfort-Geräts einzeln bestätigen:

- Betrag der Überweisung
- Kontonummer des Empfängers

Ein entsprechender Text, dass diese Angaben zu überprüfen sind, befindet sich auf der Webseite, welche den Flickercode anzeigt. Da diese beiden Ausgaben auf dem vertrauenswürdigen Display des chipTAN comfort-Geräts angezeigt werden, kann insbesondere die Kontonummer des Empfängers von einem Angreifer nicht direkt manipuliert werden, ohne dass dies dem Benutzer auffällt. Um dennoch einen erfolgreichen Angriff durchzuführen, kann der Angreifer jedoch auf Sammelüberweisungen zurückgreifen. Führt der Benutzer eine Überweisung durch, so legt der Angreifer zeitgleich im Hintergrund eine neue Sammelüberweisung an. Diese Sammelüberweisung enthält lediglich eine Überweisung auf das Konto des Angreifers, die den Betrag von der Überweisung des Benutzers übernimmt. Den aus der Sammelüberweisung resultierenden Flickercode präsentiert der Angreifer dem Benutzer statt des Flickercodes, welcher zu der ursprünglich eingegebenen Überweisung gehört. Zusätzlich passt der Angreifer den Text der Webseite an, so dass der Benutzer aufgefordert wird, den Betrag der Überweisung sowie die Anzahl der Überweisungen zu überprüfen.

Das vertrauenswürdige Display des chipTAN comfort-Geräts präsentiert nun ebenfalls Betrag und Anzahl der Überweisungen, da der Flickercode zu einer Sammelüberweisung gehört. Dies

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

ist dem Benutzer nicht bewusst. Die Ausgabe des Geräts stimmt also mit dem Text der Online-Banking-Webseite überein, so dass selbst Benutzer, denen bekannt ist, dass normalerweise die Kontonummer des Empfängers und nicht die Anzahl der Überweisungen angezeigt wird, diesen Angriff nur schwer erkennen können.

2.3 SEPA-Überweisungen

Das Zielkonto bei einer SEPA-Überweisung wird als IBAN angegeben. Diese kann eine Länge von bis zu 34 Zeichen erreichen[3]. Um die Überweisung zu autorisieren, muss der Benutzer die folgenden, über einen Flickercode auf das chipTAN comfort-Gerät übertragenen Daten bestätigen:

- Betrag der Überweisung
- Zeichen 3 und 4 sowie die letzten vier Zeichen der IBAN des Zielkontos

Auch hier befindet sich ein entsprechender Text auf der Online-Banking-Webseite, welche auch den Flickercode und die zu überprüfenden Daten enthält. Manipuliert ein Angreifer die Kontodaten und somit auch die IBAN des Zielkontos, so werden nach Übertragung des Flickercodes auf das chipTAN comfort-Gerät die oben genannten sechs Zeichen dieser neuen IBAN auf dem Display angezeigt und müssen vom Benutzer verifiziert werden. Für einen Angreifer ist es zu diesem Zeitpunkt jedoch möglich, den Inhalt der Webseite zu verändern. Er kann also auch die Anleitung zur Verifikation der IBAN manipulieren. Aufgrund der Länge der ursprünglichen, vom Benutzer eingegebenen IBAN ist es sehr wahrscheinlich, dass diese die auf dem Display angezeigten Zeichen (der vom Angreifer vorgegebenen IBAN) enthält. Der Angreifer kann also die Verifikationsanleitung so verändern, dass scheinbar die originale, vom Benutzer eingegebene IBAN verifiziert wird, indem nach den entsprechenden Positionen in der originalen IBAN gefragt wird.

Gibt der Benutzer die anschließend auf dem Display angezeigte TAN ein, kann der Angreifer den manipulierten Überweisungsauftrag gegenüber der Bank autorisieren.

3 Fazit

Das chipTAN comfort-Verfahren ist anfällig für die vorgestellten Man-in-the-Middle-Angriffe. Da bei keinem der Angriffe aber der Betrag unbemerkt von einem Angreifer verändert werden

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

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

kann, ist das Verfahren dem iTAN-Verfahren vorzuziehen. Desweiteren ist das chipTAN comfort-Verfahren im Moment noch nicht sehr weit verbreitet, so dass entsprechende Angriffe in der Praxis unwahrscheinlich erscheinen. Allerdings steigt diese Wahrscheinlichkeit, ähnlich wie schon bei der Einführung des iTAN-Verfahrens, deutlich an, sobald eine relevant große Menge von Benutzern dieses Verfahren verwendet.

Somit gefährden Man-in-the-Middle-Angriffe Bankkunden auch bei der Nutzung des chipTAN comfort-Verfahrens, auch wenn hier, anders als bei den in der Praxis bereits vorkommenden Angriffen auf das iTAN-Verfahren, der Überweisungsbetrag nicht unbemerkt verändert werden kann.

3.1 Maßnahmen durch den Benutzer

Um sich speziell vor den vorgestellten Angriffen auf das chipTAN comfort-Verfahren zu schützen, sollte der Benutzer darauf achten, dass er wirklich mit der echten Bank kommuniziert und nicht Opfer eines Man-in-the-Middle-Angriffs ist. Insbesondere muss der für das Online-Banking verwendete PC frei von Schadsoftware gehalten werden. Es zeigt sich allerdings, dass dies in der Praxis für viele Benutzer eine sehr schwierige Aufgabe ist. Werden allerdings Man-in-the-Middle-Angriffe erfolgreich vermieden, so gilt auch bereits das iTAN-Verfahren als hinreichend sicher.

Verwendet der Benutzer eine Sammelüberweisung in Verbindung mit dem chipTAN comfort-Verfahren und findet gleichzeitig ein Man-in-the-Middle-Angriff statt, so ist der in Abschnitt 2.1 beschriebene Angriff für den Benutzer nicht erkennbar.

Die vorgestellten Angriffe auf einfache Überweisungen und SEPA-Überweisungen sind hingegen für geschulte Benutzer theoretisch erkennbar. Zwar erscheinen die vertrauenswürdige Anzeige des Geräts sowie die Inhalte der angezeigten Webseite schlüssig und konsistent, dennoch könnte auffallen, dass diese Ausgaben in der Vergangenheit eine andere Form hatten.

3.2 Maßnahmen durch Banken

Als erste Maßnahme sollten Benutzer genau informiert werden, wie die Ausgaben des chipTAN comfort-Geräts bei den unterschiedlichen Transaktionen aussehen müssen. So können zumindest zwei der drei Angriffe durch entsprechend geschulte Benutzer erkannt und verhindert werden. Der Angriff auf Sammelüberweisungen ist so nicht zu erkennen. Auf Dauer sollte die Anzeige des chipTAN comfort-Geräts möglichst alle Informationen zur autorisierenden Transaktion anzeigen. So könnten alle Angriffe durch die Benutzer über die Anzeige des Geräts erkannt und somit verhindert werden.