社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (37)
2009－CSEC－ 44 (37)
2009／3／6

取引認証の改良と安全性・利便性についての考察

桜井 鐘治
三菱電機株式会社

インターネットを使った取引では、マンインザミドル攻撃や、トロイの木馬などの不正なソフトウェアを端末に送り込むことにより、利用者が意図しない取引を行う問題が指摘されている。本稿では、取引に必要な情報を携帯電話で暗号化してサーバ側へ提供し、取引実行の前に利用者がサーバ側から表示される情報をPC上で確認できるようにすることで、これら不正な取引を防止するための改良を提案する。さらに、本改良についての安全性と利便性について考察する。

Improvement of Transaction Authentication and Usability

Shoji Sakurai
Mitsubishi Electric Corporation

In transactions over the Internet, a problem that transactions which are not intended by user are done illegally by the man-in-the-middle attacks and Trojan horses on terminals is pointed out. This paper proposes an improved protocol for protection against these illegal transactions. This protocol prevents these illegal transactions by offering encrypted transactions information from user's mobile phone to a server side, and by confirming information from the server on user's PC before execution of transactions. This paper also discusses the security and usability of this proposed protocol.

1. はじめに

フィッシングが大きな社会問題になってから久しいが、金融機関などからと称して不正なサイトへの接続を促すメールを送付し利用者の静的なパスワードを盗み取って悪用する従来型のフィッシングが近年減少している一方で、利用者のPC上で動作してパスワードを不正に盗み取るキーロガーや、DNSを書き換えることにより不正なサーバへ接続させてパスワードの盗み取るファーミングなどの、より高度な攻撃手法が増加していることが報告されている[1]。さらに、これら攻撃への対策として導入されたワンタイムパスワード（以降、OTPとする）トークンに対しても、不正なサイトで盗み取ったOTPを即座に使って不正を働くリアルタイムマンインザミドル攻撃による被害も実際に報告されている[2),6)]。さらに、以前より"corrupt teller problem"などとも呼ばれてその危険性が指摘されていた問題[3]に対しても、マンインザブラウザ攻撃と呼ばれる、PCとサーバとの間で認証が確立された後に、利用者がブラウザに対して入力した振込先をサーバへの送信前に不正な口座に書き換える"Silent Banker"と名づけられたトロイの木馬が検出されたことが報告されており[4]、このマンインザブラウザ攻撃による実害の発生が懸念されている。

本稿では、この今後実害の発生が予想されるマンインザブラウザ攻撃への対策として、携帯電話を用いて振込先口座番号を入力し、取引の実行前

にサーバ側から PC の画面へ表示される情報を利用者が確認することで、不正な取引の実行を防止する方式を提案する。以降、2 章では、マンインザブラウザ攻撃による不正取引実行の流れについて記述し、3 章でこの攻撃に対する従来の不正取引対策を示し、4 章でこれらを改良した提案方式を説明し、5 章で評価を行い、6 章にまとめを示す。

2. マンインザブラウザ攻撃

マンインザブラウザ攻撃は、利用者の端末上にマルウェアとして機能するトロイの木馬を不正に送り込み、これを使って攻撃を行う。**図 1** にマンインザブラウザ攻撃の概念を示す。マンインザミドル攻撃が利用者の端末とサーバとの間の不正なサーバを使って攻撃を行うのに対し、マンインザブラウザ攻撃は、利用者とブラウザとの間でマルウェアを使って攻撃を行う。このため、SSL/TLS によりブラウザとサーバとの間にセキュアな通信セッションを確立したとしても、このセキュアな通信セッションの外側となるブラウザ上で利用者の入力する取引情報やその実行結果が不正に改ざんされる。マンインザブラウザ攻撃は、利用者が銀行のインターネットサイトへアクセスしてブラウザに振込操作が入力されるのを待ち受けて、振込先口座番号を別の口座番号に書き換えて不正な振込を実行する。この攻撃は、ブラウザのエクステンションや DLL やヘルパーオブジェクト等で実現され、実際に学部生のレベルでも実装できたことが報告されている[5]。

携帯電話による二経路認証を使った場合と、OTP トークンによる二要素認証を使った場合とに対して、マンインザブラウザ攻撃を行った場合の不正取引の流れを**図 2** と**図 3** にそれぞれ示す。なお、本稿では、取引情報の入力に先立つ利用者の本人認証は別途何らかの方法で実施されるものとする。

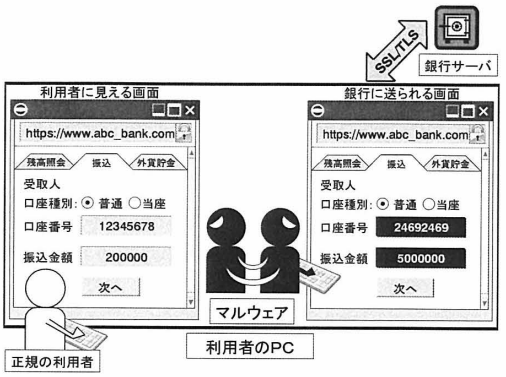

図 1 マンインザミドル攻撃の概念

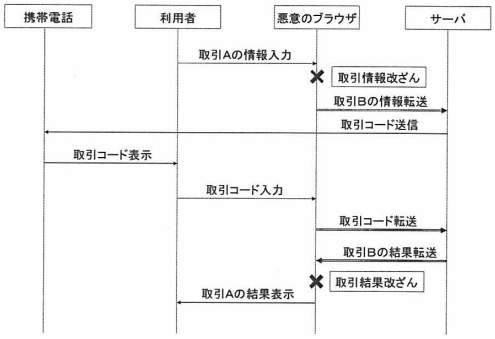

図 2 二経路認証でのマンインザブラウザ攻撃

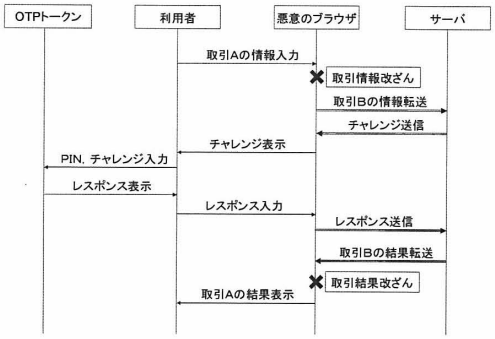

図 3 二要素認証でのマンインザブラウザ攻撃

いずれの場合においても、不正に改ざんされた取引の情報が正規の利用者の操作を行っていることを確認するために用いられる取引コードあるいはレスポンスに含まれていないため、利用者のレベルでは取引に不正に加えられた改ざんを検出することはできない。このため、このマンインザミドル攻撃に対してはこれまでに次の 3 章

に示すようにいくつかの対策が提案されている。

3. 従来の不正取引対策

3.1. 二経路認証での不正取引対策

二経路認証での不正取引対策としては、**図 4** に流れを示すような、取引コードと合わせて送信先口座の番号や金額などの利用者がブラウザに入力した取引情報を携帯電話へ送信して画面へ表示し、利用者が表示される取引の情報を確認して不正に改ざんされていることに気づいた場合には、取引コードをブラウザへ入力しないで取引を終了することで不正な取引を中止することができる対策が実施されている[7]。

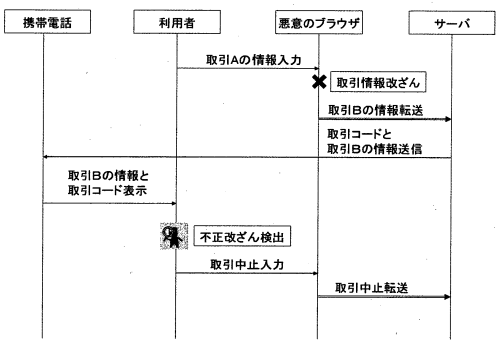

図 4 二経路認証での不正取引対策

なお、二経認証での不正取引対策は、携帯電話へ送信する情報について、送信元を詐称できないこと、送信されるメッセージが盗聴・改ざんできないことを前提としており、さらに、携帯電話については、マルウェアから隔離されたセキュアなプラットフォームであることを前提としている。

3.2. 二要素認証での対策

同様に、二要素認証においても、**図 5** に流れを示すような、取引の情報を端末に接続したトークンとサーバとの間で SSL/TLS による双方向認証を実施して確立したセッションを使って利用者がブラウザに入力した取引の情報をトークンの画面に表示し、利用者が表示される取引の情報を確認して、取引の情報が不正に改ざんされていることに気づいた場合には、トークンの中止ボタンを押下することで不正な取引を中止することができる対策が提案されている[8]。

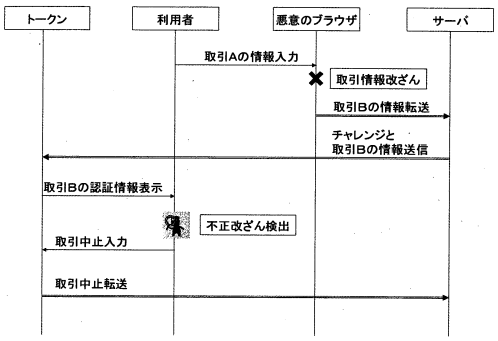

図 5 二要素認証での不正取引対策

なお、二要素認証での対策は、トークンが内部情報を取得しようとする不正な攻撃に対して耐タンパ性を保持していることを前提としている。

4. 提案方式

3 章で示した 2 つの対策は何れも、携帯電話の画面上、あるいは、トークンの画面上に取引情報（振込先口座番号と振り込み金額）を表示し、利用者が PC へ入力した取引情報と一致しているかを確認することで不正な取引の実行を防止するものである。しかしながら、入力した口座番号が改ざんされていないかを利用者に確認させる方式について行われた検証実験では、8 桁の振込先口座番号のうちの 5 桁を改ざんしても 21%の割合で振込先口座番号の確認に失敗することが報告されている[10]。これに対して本稿では、入力した口座番号に対して、PC の画面上で口座名を確認することで確認の失敗を緩和する改良方式を提案する。

図 6 に提案方式における取引の流れを示す。提案方式では、マルウェアによる不正取引を以下の手順で検出する。なお、以降では $E_K(X)$は鍵 K による平文 Xの暗号文を意味する。

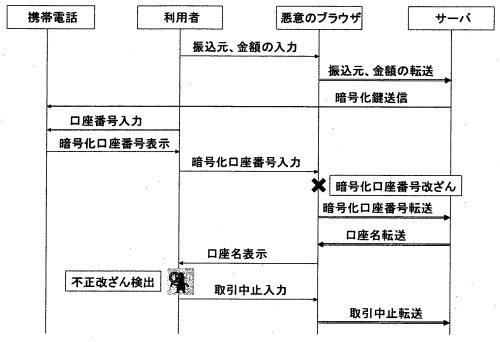

図 6　提案方式での取引の流れ

① 利用者は取引情報の内、振込元口座番号(As)と金額(M)をブラウザに入力

② ブラウザからサーバへ振込元口座番号(As)と金額(M)を送信

③ サーバから利用者の携帯電話へメールで暗号化鍵(Key)を送信

④ 利用者が携帯電話に振込先口座番号(Ad)を入力

⑤ 携帯電話の画面上に振込先口座番号を③で受信した暗号化鍵を使って暗号化した暗号化口座番号($E_{key}(Ad)$)を表示

⑥ 利用者が暗号化口座番号($E_{key}(Ad)$)をブラウザに入力（ブラウザ上でマルウェアが振込先口座番号($E_{key}(Ad)$)を改ざん）

⑦ ブラウザからサーバへ暗号化口座番号($E_{key}(Ad)$)を送信

⑧ サーバからブラウザへ口座番号に対応する口座名を送信

⑨ ブラウザ上に口座名を表示

⑩ 利用者が口座名を確認し、取引の実行／中止を入力（表示される口座名が入力した振込先口座番号に対応する口座名でない場合、あるいは、該当する口座なしと表示される場合には、取引の中止を入力）

⑪ ブラウザからサーバへ取引の実行／中止を転送

5. 考察

5.1. 安全性の考察

提案方式では、利用者からブラウザに入力される情報には、

- 振込元口座番号(As)
- 金額(M)
- 暗号化口座番号
- 取引の実行／中止

がある。これらの情報の内で、マルウェアによりマンインザミドル攻撃を実行する者が不正な振込で利益を得るためには、振込先口座番号を不正振込しようとする口座の番号へ正確に変更することが必要になる。しかしながら、ブラウザに入力される振込先の口座番号は暗号化されており、暗号化の鍵はブラウザを通過しないため、ブラウザでは正確に不正振込先の口座番号に変更することはできない。ブラウザ上のマルウェアでは、暗号化された値を適当な値に変更することできるが、この場合には、サーバで復号された口座番号には該当する口座が存在しないか、該当する口座が存在しても、攻撃者が不正に振込しようとしている口座の番号に一致することはほとんど起こり得ない。また、他の３つの入力情報については、攻撃者がマルウェアを使ってこれらの入力情報を改ざんしても、取引を混乱させたり妨害したりはできるが、目的とする不正振込を実行して利益を得ることはできない。

また、提案方式でブラウザに送信される情報には、

- 口座名

がある。口座名はサーバにおいて暗号化口座番号を復号して得られたものがブラウザに送信されるため、ブラウザでこれを受信した時には、既にサーバでは振込先口座は決定しており、マルウェアがこれを変更することはできない。このため、攻撃者はマルウェアを使って、受信した口座名を変更して取引を混乱させたり妨害したりはでき

るが、目的とする不正振込で利益を得ることはできない。

提案方式は従来の二経路認証による不正取引対策と同様に、サーバから携帯電話への秘密情報の通知を行っている。このため、次に二経路認証が前提とする条件が守られない場合を考察する。

まず、携帯電話へ送信する送信元が詐称できるとした場合には、利用者がブラウザへ振込元口座番号と金額を入力したタイミングで、マルウェアと不正なサーバとが連携し、送信元を詐称して偽の暗号化鍵を利用者の携帯電話へ送付することができる。この場合に、マルウェアは利用者が入力する暗号化口座番号を復号して振込先口座を特定することはできるが、マルウェアは正規のサーバが生成する暗号化鍵を知りえないため、不正振込をしたい口座番号を正確に復号されるように暗号化してサーバへ送付することはできない。

次に、サーバから携帯電話へ送信されるメッセージが盗聴できるとした場合には、マルウェアで暗号化鍵を使い、暗号化口座番号を復号して利用者が意図する振込先の口座番号を取得し、実際に振込を行う振込先口座とは関係なくこの口座名を利用者に表示することができる。さらに不正な振込先口座番号を暗号化してサーバへ送信することができるため、不正な振込が可能である。ただし、これには、サーバと携帯電話の間のネットワークにアクセスでき、かつ、盗聴した地点からマルウェアへ暗号化鍵をリアルタイムに通知できることが必要であり、サーバと携帯電話間がインターネットを介さないクローズドなネットワークの場合には、攻撃は非常に難しい。

最後に、携帯電話がセキュアなプラットフォームでなく、ここにもマルウェアが存在するとした場合には、利用者が入力した振込先口座番号を不正な口座に書き換えた後、これを暗号化して暗号化口座番号としてサーバへ通知することができる。ただし、この場合にもサーバ側では、復号した口座番号から口座名を取得して利用者への確認を行うため、ブラウザ側のマルウェアでは攻撃者が目的とする不正な口座への振込の確認については、利用者へは通信やシステムのエラー画面などを表示し、サーバへは実行を自動的に応答するようにすることで、不正な振込が可能である。

5.2. 利便性の考察

文献 8)では、セキュリティの利便性に関する脆弱性として、行動と判断ついて以下の各４つが提案されている。

SUV-A1：利用者が要求されているセキュリティ行動を理解できない

SUV-A2：利用者が正しいセキュリティ行動を行うのに十分な知識を持っていない

SUV-A3：セキュリティ行動の心理的または肉体的な負荷に耐えられない

SUV-A4：繰り返し行う場合に心理的または肉体的な負荷に耐えられない

SUV-C1：利用者が情報に基づく要求されたセキュリティ判断を理解しない

SUV-C2：システムが利用者にセキュリティ判断に必要とされる十分な情報を提供しない

SUV-C3：セキュリティ判断を行う精神的な負荷に耐えられない

SUV-C3：繰り返し行う場合のセキュリティ判断の精神的な負荷に耐えられない。

ここでは、提案方式における上記脆弱性を考察する。なお、3 章で紹介した対策の確認誤りが21%であったという値は、文献 8)では SUV-C3 と SUV-C4 において脆弱であるとされている。

SUV-A1 と SUV-A2 については、携帯電話と PC が普通に使えれば問題なくクリアできる。

SUV-A3 と、SUV-A4 については、暗号化口座番号の入力文字数が問題となる。実際に振込先口座を一意に特定する番号には、銀行番号 4 桁と支店番号 3 桁と口座番号 7 桁が使われており、これらを合計しても 14 桁であり、48bit で示すこ

とができる。このため、携帯電話の画面に表示する暗号化口座番号の文字数は、暗号化方式に依存するが、BASE64で、例えば、ブロック長が64bitの3DESを用いた場合には11文字、ブロック長が128bitのAESの場合には22文字となる。このため、繰り返し行う場合には、個人差はあるものの入力誤りが生じることが予想される。後の手順で口座名の確認があるため、誤った振込は防げるが、携帯電話からPCへは、何らかの手段で暗号化口座番号を受け渡すことが必要である。

SUV-C1からSUV-C4について、利用者がセキュリティ的な判断を要する点は、口座名が意図するものかの確認だけである。このため、従来方式の番号が一致しているかの確認に比べて負荷も低く、ほとんどの利用者においては繰り返し行ってもその精神的負担は低いものと考えられる。また確認はPCを使って行うため、口座名を大きなフォントを使ってテロップで表示し、テロップの表示が完了して初めて確認のボタンが押せるようにすることや、画面表示だけでなく音声でも読み上げることなどで、負担をさらに小さくできるものと考える。これらの効果を明らかにするには、今後、検証実験が必要である。

6. まとめ

不正な取引を行うマンインザブラウザ攻撃への対策として携帯電話で暗号化した振込先口座番号をサーバに提供し、ＰＣで口座名を確認することでセキュリティを高める方式を提案し、安全性と利便性について考察した。提案方式は、携帯電話網が盗聴されない場合で、かつ、携帯電話とPCとに同時にマルウェアが存在しない場合において安全性を保つことができる。利便性を高めるためには、携帯電話から暗号化口座番号の受け渡しに工夫が必要であり、利便性の効果を明らかにするためには、今後、実証実験が必要である。

参考文献

1) Anti-Phishing Work Group (APWG): Phishing Activity Trends Report Q1/2008 (online), available from <http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf> (accessed 2009-01-29).
2) ABN-AMRO: ABN AMRO intensiveert campagne voor veilig computergebruik na virusaanval op PC's klanten (online), available from <http://www.group.abnamro.com/pressroom/pressreleasedetail.cfm?ReleaseID=278555> (accessed 2009-01-29).
3) Jakobsson, M., Myers, S.: Phishing and Countermeasures, Wiley-Interscience (2006)
4) Liam O Murchu: Banking in Silence, Symantec Corporation (online), available from <https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/181> (accessed 2009-01-29).
5) Verdurmen, J.: Firefox extension security, Bachelor thesis, Radboud Universiteit Nijmegen (2008).
6) Hegt, S.: Analysis of Current and Future Phishing Attacks on Internet Banking Services, Master Thesis, Technische Universiteit Eindhoven (2008).
7) Bank Austria: mobileTAN information (online), available from <http://www.bankaustria.at/de/19741.html> (accessed 2009-01-29).
8) Weigold, T., Kramp, T., Hermann, R., Horing, F., Buhler, P. and Baentsch M.: The Zurich Trusted Information Channel - An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks, Proc. TRUST 2008, LNCS 4968, pp.75-91 (2008).
9) Josang, A., AlFayyadh, B., Grandison, T., AlZomai, M. and McNamara, J.: Security Usability Principles for Vulnerability Analysis and Risk Assessment, Proc. Computer Security Applications Conference (ACSAC2007), pp.269-278(2007)
10) AlZomai, M., AlFayyadh, B., Josang, A. and McCullagh, A: An Exprimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems, Proc. The Australasian conference on Information security (AISC2008), Australian Computer Society, Inc., pp.65-73(2008).