二段階認証の脆弱性に関する現状と課題

原 大司[1,a)]　櫻井 幸一[1,b)]

概要：現代では、様々なオンラインサービスがその利用に認証を必要としている．認証は，そのシステムが脆弱であると攻撃者による攻撃の的となる．認証システムに対し一度でも攻撃が成功すると，その被害はサービスを利用しているユーザー全体に及び，計り知れない損害を出す可能性がある．そこで，認証システムに対する攻撃手法を明らかにすることは重要な課題となっている．今利用されている認証システムの多くは二段階認証を採用している．二段階認証とは，ユーザー名/パスワードのみで認証を行なっていた従来の認証システムに追加して,SMS を利用した認証コードの入力などを用いることでもう一段階認証を追加したシステムである．この二段階認証の実装により，従来の認証システムに比べて，なりすましなどの攻撃に対するリスクが大幅に減少した．しかし，今ではその二段階認証システムでさえ攻撃者はその攻撃手法を確立し，実際に攻撃を成功しているケースが多数ある．そこで本論文では，二段階認証に対し実際に行われている攻撃手法について調査，報告し，二段階認証の安全性についての考察を行う．

キーワード：認証，リスク分析・評価，システム評価・監査，不正・異常検出

Current Status and Issues Related to Vulnerabilities of Two-Factor Authentication

DAIJI HARA[1,a)]　KOICHI SAKURAI[1]

Received: February 25, 2020, Accepted: February 25, 2020

Abstract: In modern times, various online services require authentication for their use. Authentication is targeted by an attacker if the system is vulnerable. If an attack is successful even once against an authentication system, a damage can affect an entire user of a service and cause enormous damage. Therefore, it is important to clarify attack methods for authentication systems. Many of current authentication systems adopt two-factor authentication. Two-factor authentication is a system in which authentication is added by using an authentication code input using SMS, etc. to the conventional authentication system that performed authentication only with a username / password. By implementing this two-factor authentication, a risk of attacks such as spoofing has been significantly reduced compared to conventional authentication systems. However, there are many cases where attackers have now established attack methods even with two-factor authentication systems and have actually succeeded. In this paper, we investigate and report on attack methods actually used for two-factor authentication, and consider a security of two-factor authentication, and consider a security of two-factor authentication.

Keywords: authentication, risk analysis and assessment, system evaluation and audit, fraud / abnormality detection

1. はじめに

オンラインサービスを利用する上で，認証を行うことが当たり前になってきている．認証に用いる要素として，三大要素が共通認識として存在する．それは知る要素，持つ要素，備える要素である．認証システムはこれらの要素を用いることによって認証を行う．従来の認証システムは，これらの要素のうち１つの要素のみを用いた一段階認証が主だったが，一段階認証の脆弱性を突く攻撃が激化した．そこで，現在では二段階認証を採用することが多くなった．二段階認証システムの登場により，攻撃は一時的に収まったが，今では二段階認証システムに対する攻撃例も報告され，その攻撃手法についてもよく議論に上がる．そこで本論文では，現在広く用いられている二段階認証システムに対する攻撃手法を調査，報告し，二段階認証システムの安全性についての考察を行う．

2. 認証について

ここでは認証の三大要素，認証システム，二段階認証と二要素認証の違いについて説明する．

2.1 認証の三大要素

(1) 知る要素

知る要素はよく認証に用いられる最も一般的な要素である[1]．その例としてパスワード，セキュリティ保護の質問への回答（あなたが初めて飼ったペットの名前はなんですか？等），PIN（個人識別番号）などが該当する．ユーザー名やメールアドレスはあくまで身元確認に使用するものであり，知る要素には該当しない．現在では認証を求めるサービスの増加や，サービスごとのパスワードポリシーの兼ね合いで英数字パスワードが使いにくくなってきている．知る要素はパスワードを忘れたり，メモした紙を落としたり盗まれたりするリスクが存在する．

(2) 持つ要素

この要素は携帯できるような要素を指す．例えば，銀行は送金する際にワンタイムパスワードにより生成されるトークンを要求する．このトークンは RSA の Secure ID などにより生成される．ワンタイムパスワードには HOTP と TOTP の二種類がある．HOTP はユーザーが使用するまで有効期限が残るトークンであり，TOTP はパスワードを発行して 30 秒で有効期限が切れるトークンである．持つ要素は，パスワード生成機の故障や紛失のリスクが存在する．

(3) 備える要素

生体認証に用いる要素である．各個人が持っている，他の誰とも被らない情報である．例えば，指紋，掌紋，声紋，網膜，虹彩，顔などが該当する．この要素は他の要素に比べて紛失や盗難のリスクが無く，安全な要素と言える．しかし，生体情報の読み取り機が必要になるため，導入のためのコストが高いことが欠点である．

(4) その他の要素[2]

ここで紹介する要素は，世間の認証で目にする機会は少ないが，研究対象として注目されている要素である．まず，「位置的要素」である．この要素で最も一般的なものは IP アドレスである．普段ログインを行なっている IP アドレス以外でのログインの試みがあった場合通知を行い，ログインの許可を行うか認証を行う．他の要素としては MAC アドレスもここに該当する．他に「行動的要素」も存在する．これは紹介した中でも最も用いられていない要素である．ジェスチャーなどのアクションを観察することで身元を証明する認証に用いられる．Windows8 の Picture Password がこれを採用している．

2.2 認証システム

従来の単一認証では，パスワードの漏えいや総当たり攻撃での推測成功などによって簡単になりすましが成功していた．そこで二段階認証を導入することで，パスワードが割れても二段階目の認証でなりすましを防ぐことができる．

１つの認証システムには主要認証と緊急認証が存在し，それぞれ役割が異なる．

(1) 主要認証

この認証は一般的な過程でユーザーが最初に行う認証である．この認証に失敗した場合，緊急認証に移行する．

(2) 緊急認証

緊急認証はユーザーが主要認証に失敗した場合に行われる保険のような役割を担う認証である．攻撃者は認証システムの最も脆弱な点を狙って攻撃を行うため，緊急認証であっても主要認証と同程度のセキュリティレベルが必要になる．

2.3 二段階認証と二要素認証の違い

二段階認証と二要素認証は，どちらも従来の単一認証の脆弱性を改善するために登場したものである．しかし，それぞれ一見似ているようで明確に異なる．その違いは，認証プロセスが二段階に分かれているか否かである[3]．今よく用いられている SMS を用いた二段階認証を考える．これはまずユーザー名/パスワードを入力する（一段階目）．その後登録していた電話番号宛に SMS が送信されるので，そこに記されているコードを入力する（二段階目）．二要素認証は，その認証に用いる要素の種類が被ってはいけない．つまり，前述した三大要素（ + その他の要素）の組み合わせで行わなければならない．例えば「知る要素 + 持つ要素」や「知る要素 + 備える要素」などである．ここで注意すべきことは，「知る要素 + 知る要素」や「持つ要素 + 持つ要

1 九州大学 大学院システム情報科学府
Department of Informatics Graduate School of Information and Electrical Engineering, Kyushu University

a) daiji.hara@inf.kyushu-u.ac.jp
b) sakurai@inf.kyushu-u.ac.jp

素」は二要素認証ではないということである[4]. ここまでの例で分かるように, 二段階認証の場合は同一種類の要素を用いても良い. しかし, NIST はこのセキュリティの頑丈性を認めていない. 重要であることは, 二段階認証に用いられている要素が二要素であるか否かである.

3. 二段階認証の問題点

従来の単一認証の脆弱性を改善するために導入された二段階認証であるが, その二段階認証にも多くの問題点があることが判明した. 例えば SMS を利用した二段階認証が現在多く用いられているが, この認証方法はスマートフォンの紛失や盗難によるリスクを抱えている. また, その他にも二段階認証に対する多くの攻撃手法[5]が判明し, 実際に成功している. この章ではその攻撃手法を紹介する.

3.1 キーロガーによるパスワード漏えい

キーロガーとは, PC 使用者がどのようなキーボード入力を行なっているかを記録するアプリケーションである. 使用例としては, 従業員の作業効率を監視するために用いるなどが挙げられる. キーロガーは認証の要素に知る要素を用いている場合に効果的な攻撃手法である. 攻撃者はキーロガーを攻撃対象の PC に仕込んでおく. その PC ユーザーがパスワードを入力した際に入力情報が攻撃者に取得されるというものである[6]. 二段階認証の要素が知る要素のみで構成されている場合, このアプリケーションのみで容易に攻撃が成功する. この攻撃は, 二段階認証の要素に持つ要素, 備える要素を用いることで防御することができる.

3.2 MITM（Man-In-The-Middle）攻撃

MITM 攻撃[7]はネットワーク通信の間に攻撃者（中間者）が不正な手段用いて割り込むことで通信内容の盗聴や改ざんを行う攻撃である[8]. MITM 攻撃は通常暗号化ネットワークプロトコル（SSL/TLS）を用いることで防御することができる. しかし, SSL 認証局が攻撃を受け, 証明書が偽造される事件も起きている. MITM 攻撃が成功した場合, 被攻撃者はその攻撃に気づくことが難しく, 通信内容が筒抜けになってしまう. 認証に知る要素のみを用いている場合この攻撃によって容易になりすましが成功してしまうため, 二段階認証の要素に持つ要素, 備える要素を用いる必要がある.

3.3 MITB（Man-In-The-Browser）攻撃

MITB 攻撃は, 攻撃対象をマルウェアに感染させ攻撃対象のブラウザを偽造する攻撃である. 特に, その攻撃対象としてインターネットバンキングを利用する顧客が標的にされる. この攻撃は Timothy Dougan らによって報告されている. [9] 攻撃者は正規サイトに精巧に似せた偽造サイトを被攻撃者に提示する. 被攻撃者は, 自分が見ている Web サイトが偽造サイトだと気付かずに, ユーザーID/パスワードを入力する. 攻撃者は正規サイトにアクセスし, 偽造サイトに入力された情報を入力する. このサイトが二段階認証を SMS で行なっている場合, 攻撃者は正規サイトに正しいユーザーID/パスワードを入力しているため認証コードが正常に被攻撃者に送信される. 被攻撃者は届いた SMS 認証コードを偽造サイトに入力するため, 攻撃者は入力された SMS 認証コードを正規サイトに入力してなりすましを完了することができる. この攻撃は上記の手順により知る要素（ユーザーID/パスワード）と持つ要素（SMS 認証コード）を組み合わせた二段階認証に対して攻撃が成功する点で他の攻撃と比較して危険度が高い.

3.4 緊急認証の脆弱性

前章で記述したように, ユーザーがパスワードを忘れたり, ワンタイムパスワードを生成できなくなったりして主要認証が行えなくなった場合に, 緊急認証に移行する. この時の緊急認証に二段階認証を用いていない場合, ソーシャルエンジニアリングなどにより, 攻撃者は簡単になりすましを完了することができる. この緊急認証に「最初に買ったペットの名前はなんですか？」などの知る要素を用いている場合, 攻撃者は SNS を利用して容易にアカウントを乗っ取ることができる. この脆弱性を考慮して, 緊急認証には知る要素を使用しないほうが良いが, ワンタイムパスワード生成機の故障や紛失により持つ要素での認証が出来ないため, 緊急認証に移行していることが考えられる. その場合は備える要素での認証を行うことが望ましい.

3.5 サードパーティー攻撃

認証システムの中には, トークンの発行や検証, または検証に伴う通信を第三者機関に依存しているものもある. この脆弱性は 2011 年に起こった RSA の Secure ID システムが侵害されたことで有名である[10]. この攻撃に成功した攻撃者は偽造トークンを生成してアカウントの乗っ取りを簡単に行えたことが予想できる. また, 二段階認証に携帯電話番号を利用した SMS コードを利用している場合, その送信先電話番号の割り当ては携帯会社に依存していることになる. 攻撃者は電話会社に携帯電話を紛失したと虚偽の申告を行い, SMS メッセージを傍受することができる. これにより二段階認証の二番目の要素を盗まれる可能性がある. 銀行などの致命的な個人情報に関わるアプリケーションには SMS を使用しないことが望ましく, 備える要素での認証を用いた方が良いことがわかる.

3.6 Smudge Attack

パスワードを認証の知る要素として用いることに対して, 最近ではその脆弱性, 利便性により疑問視されている. その代替案として図形要素を認証の知る要素として用いることが推奨されることがある[1]. 図形要素とは, スマートフォン等のタッチスクリーンに対して, あらかじめ登録していた通りに指でなぞることで本人を確かめる, 知る要素のことである. しかし, この要素に対して有効な Smudge

Attack が Adam J. Aviv らによって報告されている[11]. この攻撃はタッチスクリーンを人がなぞる際に付着する油性残留物を観測することで, ユーザーのなぞるパターンを解析する攻撃手法のことである. 油性残留物がスクリーンに存在する場所と存在しない場所では光の反射特性に違いが生じる. それを観測することでこの攻撃は達成されてしまう. 知る要素として最も一般的であるパスワード認証の利便性, 脆弱性を考慮した代替案として提案される図形要素であるが, この要素に対しても有効である攻撃手法が存在することがわかった. このことから, 認証の要素として知る要素を用いることは賢いとは言えないことがわかる.

4. 二段階認証の安全性考察

これまで記述してきた事柄をまとめると, 二段階認証は安全であるとは言えない. しかし, これを三段階認証にした場合にセキュリティレベルが格段に上がるとは考えられない. 何故ならば, 前述した通りに多段階認証を行う場合, その認証に用いる要素に別の種類のものを用いなければ十分なセキュリティレベルの向上が認められないからである. また, 認証の段階数を増やしていくことで生じるユーザビリティの低下も考えなければならない. 現在よく目にする, SMS コードを用いている知る要素 + 持つ要素で構成された二段階認証では MITB 攻撃などを防ぐことはできない. このような攻撃は, 認証の要素に備える要素を用いることで防御することができるが生体認証の導入にはコストがかかることが問題である. また, 生体認証を用いている認証システムでも, その緊急認証に生体認証を用いていない場合, 攻撃者はその脆弱性を狙って攻撃を行う. このことを考えた場合に, 緊急認証にも生体認証を取り入れた方が良いことがわかる. しかし, 常に生体認証が行える環境が整っているとは限らない. その場合に注目されるのが第四, 第五の認証要素である, 位置的要素と行動的要素だ. 位置的要素は IP アドレスや MAC アドレスによる認証要素のことである. しかし,IP アドレスは Betternet Unlimited Free VPN Proxy[12]や Hotspot Shield[13]などのアプリケーションで簡単に偽装できる. さらに MaC アドレスは iproute2[14]や macchanger[15]などで簡単に偽装することが可能であり, 暗号化されていない通信経路などから MaC アドレスを特定されると, 簡単に認証が破られてしまう[16]. 行動的要素はジェスチャーなどのアクションにより行われる認証に用いられる. この要素は他人になりすまされ難い行動を設定することで, 備える要素に次いで頑丈な要素になり得る. しかし, 完璧に一個人を特定するような行動の設定は難しく, 今様々な研究が行われている要素である.

5. おわりに

この論文では, 認証に用いられる要素, 認証システム, 二段階認証と二要素認証の違いについて説明を行った. また二段階認証が抱える問題点を, 実際に行われている攻撃手法の説明を交えながら報告した. 最後にこれらの攻撃手法から二段階認証システムの安全性について考察を行った. その結果, 現在最も良く用いられている SMS 認証コードを用いた二段階認証は今となっては頑丈と言えないことが判った. 二段階認証には備える要素を用いた生体認証を行うべきであるが, コストの問題でそれが難しい場合もある. そこで, 一個人を完全に保証できるような行動的要素の考案が重要であることが判った.

参考文献

[1] “Security and Usability in Knowledge-based User Authentication: A Review”, Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, George Samaras, ACM International Conference Proceeding Series, 20th Pan-Hellenic Conference on Informatics, PCI 2016
[2] The Five Factor of Authentication https://medium.com/@renansdias/the-5-factors-of-authentication-bcb79d354c13
[3] 二要素認証と二段階認証の違い https://www.segunabe.com/2018/08/31/passclipnews180831/
[4] 二段階認証とは https://cybersecurity-jp.com/security-measures/29203
[5] Five Most Common Security Attacks on Two-Factor Authentication https://www.itbusinessedge.com/slideshows/five-most-common-security-attacks-on-two-factor-authentication-05.html
[6] キーロガーとは？ https://cybersecurity-jp.com/security-measures/23974
[7] “Man-in-the-middle-attack: Understanding in simple words”, Avijit Mallik, Abid Ahsan, Mhia Md. Zaglul Shahadat and Jia-Chi Tsou, International Journal of Data and Network Science 3 (2019) 77–92
[8] 中間者攻撃 https://jp.globalsign.com/blog/articles/maninthemiddleattack.html
[9] “Man in the Browser Attacks”, Timothy Dougan, Kevin Curran, International Journal of Ambient Computing and Intelligence, 4(1), 29-39, January-March 2012
[10] RSA explains how attackers breached its systems https://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/
[11] “Smudge Attacks on Smartphone Touch Screens”, Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, Jonathan M. Smith, Department of Computer and Information Science – University of Pennsylvania
[12] Betternet Unlimited Free VPN https://betternet.softonic.jp
[13] Hotspot Shield https://www.hotspotshield.com/ja/
[14] iproute2 https://www.archlinux.jp/packages/?name=iproute2
[15] macchanger https://www.archlinux.jp/packages/?name=macchanger
[16] MaC アドレス偽装事例 https://www.ctcsp.co.jp/itspice/entry/032.html