G-17

ウェブアクセスにおけるパケット到着時間特性を用いた携帯電話特定方式

Identifying cell phone by using packet arrival time characteristics in web access

○相良澪[1]、児玉賢祐[1]、木原雅巳[2]
Mio Sagara[1], Kensuke Kodama[1],Masami Kihara[2]

Abstract: A new two-step authentication method for cell phones is proposed. The proposed method can identify the target user's cell phone in web access without sending or receiving one-time passwords. This system eliminates the computer virus risk. User authentication, equivalent to cell phone identification, is achieved by measuring the packet arrival time difference in web access when the cell phone receives an incoming call from the authentication server. The proposed method can be implemented by service providers themselves and its key attribute is simple implementation.

１．はじめに

本研究では、利用者認証を、利用者の携帯電話を介して行うための携帯電話特定方式においての、特定制度について述べる。利用者の携帯電話を認証デバイスとして使用し、その携帯電話と認証サーバ間の伝統遅延特性を利用する認証方式の研究を進めている。携帯電話を通して利用者の特定、認証を行う。

２．研究目的

正規利用者の ID/パスワード（以下、PW）が盗まれた場合にも正規利用者本人であることを確実に特定出来、かつ、サービス提供者が求めるタイミングで常に認証を行える個人認証方式の提案を行うことである。

３．研究背景

本研究は、利用者のコンピュータがウィルス感染し、最悪、ウィルスがブラウザに寄生して、ブラウザが処理する情報を不正に操作できる状況でも、利用者を特定し、ネットワークサービスの処理が改ざんされないようにすることを目的としている。

近年、ネットバンキングなどの金銭のやり取りを含む多くのネットワークサービスの利用が増えている。それに伴い、サーバ犯罪も増加している。このような金銭のやり取りを含むコンテンツでは、より高度な認証が求められるようになっている。そこで用いられるようになったのが ID・PW の認証に加えて、携帯電話を利用した二段階認証である。

現在の二段階認証は、ワンタイムパスワードが携帯電話に送られてくる形が一般的である。しかし、この方法だとパソコンがウイルス感染してしまった場合、特に、ブラウザがウイルス感染した場合にはウイルスの改ざんなどに対抗することが難しい場合がある。ネットバンキングで振り込みを行う場合、ユーザ認証後に、ウイルスにより振り込み先が変更されたときなどが主な例である。内容を確認するデバイスも同じであるため、振込先が変更されたことに気づくことができない。従来の方式では、ID・PW が盗まれた場合には有効であるが、要求した処理が書き換えられてしまうとその処理を止めることができない構成になっている。

４．提案方式の認証プロセス

本論文で提案する認証のプロセスを図 1 に示す。パソコンからログイン後、携帯電話からもログインを行う。ログイン後、認証用 HTML に接続することで携帯電話認証が始まる。携帯電話認証により携帯電話が利用者本人のものであると認証されるとパソコンからサービスを要求することができる。この方式は、パソコンと携帯電話が独立したプロセスで認証を行っている。そのため、二段階認証ができるだけでなく、パソコンがウイルス感染した場合にも有効な認証方式である。

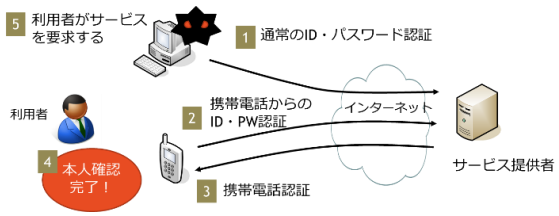

図 1　認証プロセス

５．携帯電話認証

携帯電話認証は、図 2 のような HTML ページに接続することで始まる。この HTML には数百個の画像が埋め込まれている。この画像の GET リクエストなどのパケットがサーバに到着した時点でタイムスタンプを記録する。この様子を図 3 に示す。このタイムスタンプの差分を伝送遅延として利用する。この HTML ページへアクセス中に携帯電話にサーバ側から電話をかける。

１：日大理工・学部・情報　２：日大理工・教員・情報

この電話着信により、伝送遅延が大きくなり、この遅延特性を認証に利用する。

6．伝送遅延特性の変化

実際に伝送遅延時間の測定を行った。その結果を横軸をパケット到着時間差のデータ番号、縦軸を伝送遅延としてまとめたものを図 4、図 5 に示す。図 4 は、約 2000 個のパケットの到着時間差を表している。時間差の最大値は約 22[ms]である。これに対してサーバ側から認証要求をしている携帯電話に電話発信すると、着信時に約 6.5[s]の時間差が発生していることがわかる。

本論文の提案方式は、図 4、図 5 に示した電話着信前後の伝送遅延特性に依存している。さらに、サービスサーバでのパケット到着時間は、携帯電話の伝送速度に依存する。基地局の混雑状況により、伝送速度が変化したときの電話発信前後の最大伝送遅延を図 5 に示す。30Mbps までの電話着信前後の到着時間差には、約 4[s]の差があり、安定に電話着信時の到着時間差を検出できることを示している。この電話着信が起きたタイミングで遅延が起きることを利用して利用者の携帯電話を特定することができる。

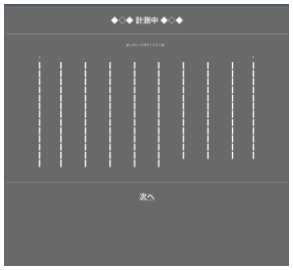

図 2　HTML ページ

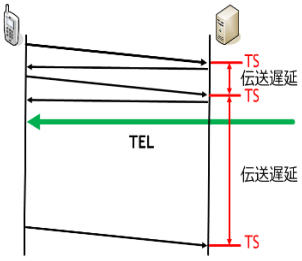

図 3　パケット到着

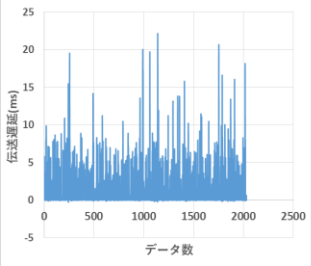

図 4　伝送遅延特性

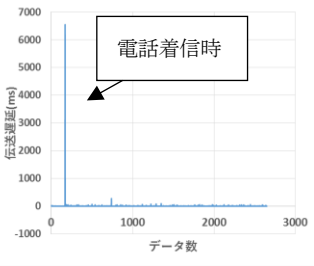

図 5　着信時伝送遅延特性

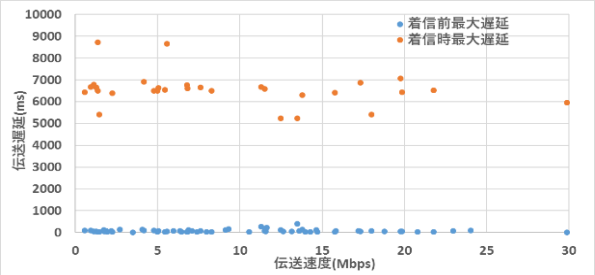

図 6　電話発信前後の最大伝送遅延

7．正規利用者の識別

携帯電話認証による正規利用者識別方法について図 7 に示す。正規利用者の電話番号と ID・PW は、サーバのデータベースで紐づけられて登録されている。サーバはユーザのログイン時の ID・PW によって電話番号を知ることができる。サーバは、認証ページにアクセスされると、ID・PW と紐づけられた番号に電話をかける。このときの到着パケット時間差に、図 5 の伝送遅延特性が現れることで携帯電話認証をすることができる。不正利用者が正規利用者の ID・PW でログインすると、サーバは ID・PW に紐づけられた正規利用者の番号に電話をかける。不正利用者の携帯電話には電話着信が起きないため、不正利用であると判断できる。このとき、正規利用者は自身が認証を行っていないのに電話がかかってくるため、不正ログインが行われたことを知ることができる。この時点で流出した PW の変更を行うこともできる。

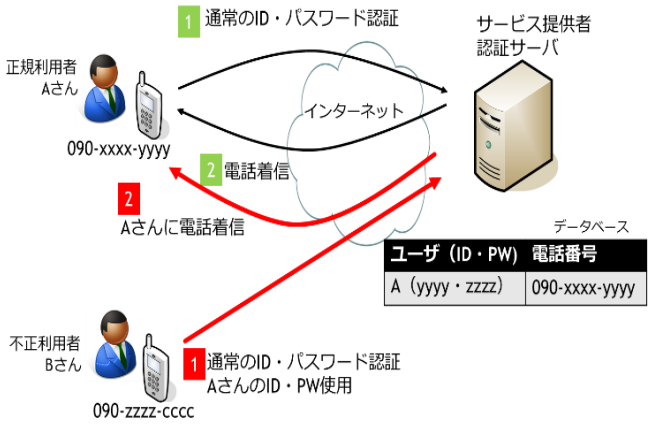

図 7　正規利用者識別方法

8．まとめ

新しい携帯電話を用いた個人認証方式の提案を行った。今後は、現在利用しているような特殊な HTML ページではなく、どのような HTML ページにも埋め込むことができる認証方式の検討を行う。また、機種やブラウザの違いによる影響についても調査予定である。

9．参考文献

[1] 寺本, 木原,"ウェブアクセス時の伝送遅延特性を用いた携帯電話認証", 2014 年電子情報通信学会通信ソサイエティ大会, B-6-47, 2014

[2] http://support.google.com/accounts/answer/180744?hl=ja