プレスリリース 2007.03.23

Yahoo! JAPAN、産業技術総合研究所と抜本的なフィッシング詐欺防止技術を開発
～ウェブに適したパスワード相互認証プロトコル～

2007年3月23日

ヤフー株式会社

Yahoo! JAPAN、産業技術総合研究所と抜本的なフィッシング詐欺防止技術を開発

～ウェブに適したパスワード相互認証プロトコル～

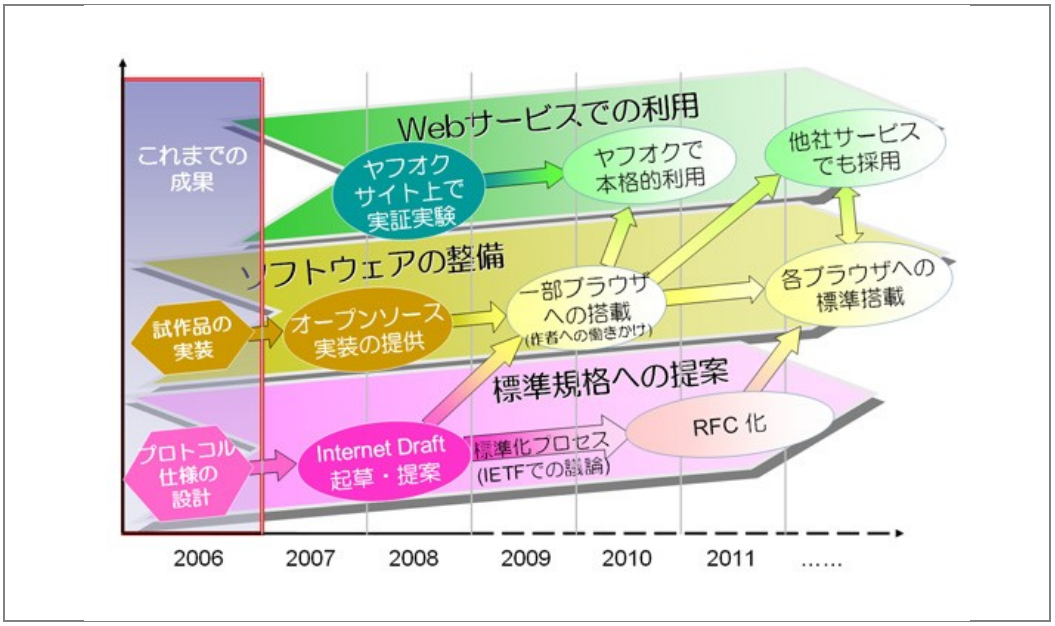
ヤフー株式会社（代表取締役社長：井上 雅博、以下「Yahoo! JAPAN」という）は、独立行政法人 産業技術総合研究所（理事長 吉川 弘之、以下「産総研」という）情報セキュリティ研究センター（センター長：今井 秀樹）と2006年1月から進めてきたインターネットにおけるセキュリティ強化技術の共同研究の成果として、ウェブでの利用に適したパスワード相互認証プロトコルを開発しました。

本技術は、近年インターネット利用の安全を脅かすものとして社会問題となっているフィッシング詐欺と呼ばれる手口に対して、パスワードや個人情報を詐取される被害を防止するための抜本的な解決策です。PAKE（*1）と呼ばれる暗号・認証技術に新たな手法で改良を加え、ウェブの標準プロトコルであるHTTPおよびHTTPSに適用したもので、ユーザーがパスワードでサイトの真偽性を確認できる仕組みを提供することによりフィッシングを防止します。偽サイトで誤ってパスワードを入力してもパスワードそのものを詐取されることはなく、ログインが成功したように偽装されることもありません。また、従来の対策手法では解決されていなかった、偽サイトが通信を本物サイトへ中継する中間者攻撃（*2）と呼ばれる手口にも対応し被害を防止します。

これまでにプロトコル仕様の設計を終え、本技術を実装したサーバーモジュールとブラウザ拡張機能を試作しました。2007年度中に「Yahoo!オークション」上での実証実験を行い、実際の運用に耐え得る仕組みであることを検証します。今後、本プロトコル仕様のRFC（*3）化に向けた手続きとしてインターネットドラフトを起草し、将来的には、オープンソースコミュニティにソースコードを提供して、ウェブにおけるパスワード相互認証の技術標準としての確立を目指します。

また、本共同研究ではその他に、フィッシング詐欺に遭わないための安全なウェブ利用の方法などについて解説した啓発コンテンツ「Yahoo!オークション 安全対策研究所」を制作し、Yahoo!オークションのサイトで順次公開しています。

両者は今後も共同研究を継続し、安全・安心なIT社会実現への貢献を目指します。



これまでの成果と今後の展開イメージ

共同研究・啓発活動の成果

（1）「Yahoo!オークション 安全対策研究所」の制作

Yahoo! JAPANは、産総研情報セキュリティ研究センター監修によるユーザー向けの啓発コンテンツとして「Yahoo!オークション 安全対策研究所」を順次公開しています。インターネットを利用する際の安全上の注意点を読み物として、具体的事例を交えて初心者にもわかりやすく提供しています。2007年3月までに、「オークション振り込め詐欺」「オークションを偽装したフィッシング」「オークション不正ID利用詐欺」「オークションの詐欺事例」をテーマにしたケーススタディを公開しました。

「Yahoo!オークション 安全対策研究所」のアドレス：
http://special.auctions.yahoo.co.jp/html/anzen/

（2）ウェブに適したパスワード相互認証プロトコルの研究開発

社会的背景

インターネットではここ数年、フィッシング詐欺と呼ばれる手口で、個人情報やパスワード等を詐取しようとする悪質な行為が横行し、社会問題となっています。フィッシングの被害に遭わないためには、ユーザーが個人情報等を入力する際に、ブラウザのアドレス欄に表示されたアドレスが自分の意図したサイトのアドレスに一致しているかを目視で確認することが基本ですが、現実には経験豊富なユーザーでもうっかり確認を怠ることがあり、また、本物とまぎらわしい名前のドメイン名で偽サイトが設置されていると目視確認では見分けにくいという問題がありました。

ウェブで利用できる従来の認証技術としては、SSLのクライアント認証方式がありました。ク

ライアント認証を用いればパスワードをサーバーに送信することがないため、フィッシングによってパスワードを詐取されることはありませんが、この方式では事前にユーザーに電子証明書を配布する必要があり、導入コストの高さや使い勝手の悪さから、公衆向けサービスでの導入事例はほとんどなく、普及していないのが実情です。

一方、近年、フィッシング詐欺対策としてワンタイムパスワードをユーザーに利用させる手法が普及しつつありましたが、ワンタイムパスワードを用いるだけでは中間者攻撃によるフィッシングの手口に弱いという問題点が指摘されていました。この懸念は、2006年7月、ワンタイムパスワードを採用していた米国の大手銀行で中間者攻撃によるフィッシングの被害が明るみに出たことで現実のものとなり、抜本的な技術的解決策が求められているところです。

研究の経緯

産総研は、2005年4月に情報セキュリティ研究センターを新設し、暗号・認証技術に関する基礎研究とインターネットの利用を安全にするための実践的研究を平行して進めてきました。一方、Yahoo! JAPANは、「Yahoo!オークション」における不正登録や不正出品の防止対策などを進めてきました。2006年1月両者は、フィッシング詐欺を防止するための新しいセキュリティ技術の開発を目指して共同研究を行うことに合意し、これまで、パスワードを用いた相互認証プロトコルをウェブに適用する方法について検討してきました。

今回、産総研の持つ次世代の暗号・認証技術に関する知見をウェブシステムに応用することにより、フィッシング詐欺によるパスワードおよび個人情報の盗難を防ぐ新しい認証プロトコルを発案するとともに、Yahoo! JAPANの持つ大規模サイトの運用に関するノウハウを参考に、様々な利用形態に対応できるよう配慮した実用的なプロトコルとして設計し、サーバーモジュールとブラウザ拡張機能の試作を行いました。

開発の内容

1. PAKE方式の採用

今回開発したプロトコルは、PAKE（Password Authenticated Key Exchange）方式のひとつであるISO/IEC 11770-4のプロトコルを基盤として設計しました。PAKE方式を採用することで、ユーザー固有のパスワードによる相互認証を実現することができます。ユーザーにとっては使い慣れたIDとパスワードを利用するだけでよく、サービス提供者はユーザーに新たな負担を強いることなく導入できる相互認証方式です。

この方式では、ユーザーにより入力されたパスワードは乱数を用いて暗号学的に加工された情報としてサーバーに送信され、一方サーバー側は、そのユーザーのパスワードとして事前に登録されている情報を加工してユーザーのコンピューターに返します。両者は暗号学的な方法でそれらの情報を検証することで、互いにそのパスワードが正しいかを検証します。サーバーがユーザーの入力したパスワードが正しいかを検証するのは従来通りですが、それだけでなく、ユーザー側は、そのサーバーが自分のパスワードを過去に登録したサーバーであるかを検証します。

2. PAKEによるフィッシング防止効果

PAKE方式による認証では、パスワードは暗号学的に加工された情報として送信されるため、もしユーザーが誤って偽サイトで送信しても、パスワード自体を盗まれることはありません。また、偽サイトに送信した場合、偽サイトはそのユーザーのパスワードを知っていないため、辻褄の合う情報をユーザーに返すことができず、認証は成功しない結果となります。そのため、ユーザーは、正しいパスワードを与えても認証が成功しない場合はそのサーバーが偽サイトである（正確には、過去に自分がパスワード登録したサーバーではない）と判別することができます。

昨今のフィッシング詐欺では偽の認証処理を行ってみせる手口が横行しています。すなわち、偽サイトはユーザーにパスワードの入力を求め、パスワードが正しいか否かにかかわらず次の画面を表示して、クレジットカード番号や個人情報などを入力させるという手口です。ユーザーは、ログインした後に情報を入力していると錯覚してしまい、偽サイトであることに気づかないことがあります。ここで、PAKE方式による相互認証プロトコルが用いられていれば、パスワードを入力しても偽サイトでは認証が成功しないため、そうした錯覚を防止することができます。

この性質は、従来のSSLクライアント認証でも達成していなかったフィッシング防止に適した特長です。

3. HTTPアクセス認証との融合

従来のPAKE方式では、相互認証後に通信データの暗号化も施すのが一般的な使い方ですが、今回、ウェブへの適用にあたって、データの暗号化にPAKEは用いない方針をとりました。これは、ウェブにおける暗号化通信はSSLを用いたHTTPSプロトコルが標準となっており、既にユーザーにも広く認知されているところ、新たに別の暗号化方式が加わることは、ユーザーを混乱させ、正しい使い分けを難しくすると判断したためです。データの暗号化が不要な場合はHTTPとPAKEを組み合わせて用い、暗号化が必要な場合はHTTPSとPAKEを組み合わせて用いることにしました。

具体的には、HTTPアクセス認証(RFC 2617) の自然な拡張として設計し、Basic認証、Digest認証と同じフレームワークを利用した“Mutual”認証を新たに開発しました。この設計にあたっては、ロードバランサーやSSLアクセラレーター等の既存の技術との親和性に配慮し、提案技術がスムーズに普及するよう工夫しました。

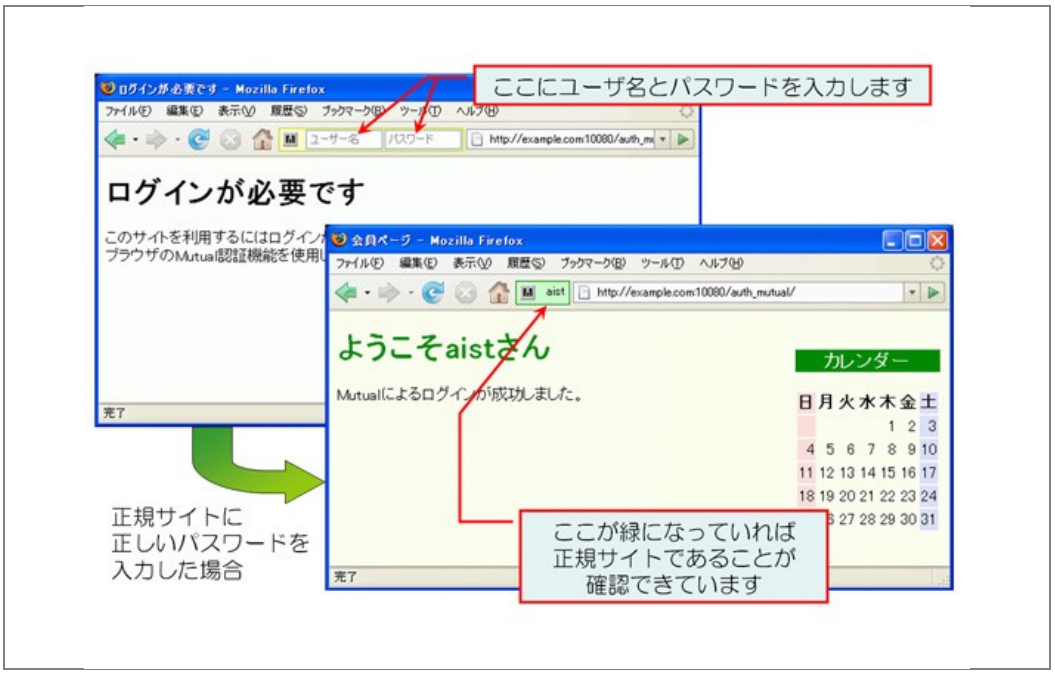
4. 中間者攻撃の回避

なお、このような設計では中間者攻撃によるフィッシングの手口が問題となります。偽サイトがユーザーとの通信を本物サイトに中継する手口を用いている場合、PAKEによる相互認証は成功してしまうため、ユーザーが偽サイトと気づかずに利用を続けてしまうと、通信データを傍受されたり改ざんされる危険にさらされます。この脅威はHTTPSと組み合わせた場合であっても防止できません。そこで本研究では、PAKEプロトコルにおいてパスワードを暗号学的に加工する際に、通信相手となるサーバーのドメイン名等を使って加工するよう改良した新しいプロトコルを開発しました。これにより、偽サイトが本物サイトに中継する中間者攻撃が行われていても、認証は成功せず、ユーザーは偽サイトだと気づくことができます。

5. ユーザーインターフェイス設計

このプロトコルを実装したウェブブラウザの様子を図に示します。認証が必要なウェブサイトにアクセスすると、ユーザー名とパスワードの入力欄がブラウザのツールバー領域に現れます。偽サイトが偽の入力欄を偽装することができないよう、パスワード入力欄をツールバー領域に設けています。正しいパスワードを入力してボタンを押すと、入力欄のあった部分が緑色の表示となり、ログイン中のユーザー名を表示します。

ユーザーの使い方は次のようになります。ユーザーはパスワードをツールバー領域で入力するようにします。その結果、緑色の表示となればそれは本物サイトであると判別し、緑色にならないときは、パスワードの入力ミスであるか、または偽サイトに誤って接続していると判別します。



本技術を実装したウェブブラウザの様子

今後の予定

2007年度中に「Yahoo!オークション」上での実証実験を行い、実際の運用に耐えられる仕組みであるかを検証し、問題点の洗い出しと改良の開発を継続します。また、本プロトコル仕様のRFC化に向けた手続きとしてインターネットドラフトを起草します。将来は、オープンソースコミュニティにソースコードを提供して、ウェブにおけるパスワード相互認証の技術標準としての確立を目指し、誰もが自由に利用できる技術として広く普及することを期待します。

（*1）PAKE (Password Authenticated Key Exchange)
ISO/IEC、IEEE、IETFなどの国際標準にも採用されている、クライアント・サーバー間で相互認証とそれに基づいた秘密情報の安全な共有を実現する方式。電子証明書を用いずにユーザー固有のパスワードを用いた相互認証が可能。従来、ウェブに適用して用いられることはなく、普及が進んでいなかった。

（*2）中間者攻撃 (Man-in-the-middle Attack)
クライアントとサーバー間に割り込んだ攻撃者が、クライアントと攻撃者間の通信を攻撃者とサーバー間の通信として中継することによってセキュリティを破る攻撃手法の名称。いくつかのプロトコルはこの攻撃に対して弱いことが知られている。フィッシング詐欺においては、偽サイトでユーザーに入力させたパスワードを本物のサイトに中継する攻撃手法を指す。ワンタイムパスワードを使用していても、その時点で有効なワンタイムパスワードを偽サイトがサーバーに対して使用することができてしまうため、ワンタイムパスワードによるフィッシング対策は中間者攻撃に弱いと指摘されている。

（*3）RFC (Request for Comments)
インターネットで使用される技術の標準化作業を担う組織 IETF (Internet Engineering Task Force)が発行する文書。インターネットドラフトはIETFにおける標準化過程の最初のステップのひとつで、誰でも作成し提出することができ、一定期間公開されて意見募集の対象となる。標準化の価値があると見なされれば、「標準への提唱」（Proposed Standard）に格上げされRFCの番号が付与され、さらに「標準への草稿」（Draft Standard）を経て「標準」（Standard）となることがある。

【Yahoo! JAPAN】http://www.yahoo.co.jp/

ヤフー株式会社（市場名：東証1部/JASDAQ、銘柄コード：4689、本社：東京都港区、設立年月日：1996年1月31日、代表取締役：井上雅博）が運営するYahoo! JAPANは、1か月あたり約4,671万人のユニークカスタマー数（※1）と、1日13億7000万ページビュー（※2）のアクセスを誇るインターネットの総合情報サイトで、検索、コンテンツ、コミュニティー、コマース、モバイルなど多くのサービスを提供しています。

（※1）2007年1月のNielsen//NetRatings「NetView AMS JP」における家庭からの視聴率88.2%、職場からの視聴率91.5%というデータをもとに、家庭、または職場からのインターネットユーザーを約5,284万人（NetRatings Japan「インターネット基礎調査」より）としてYahoo! JAPANのユニークカスタマー数を算出。

（※2）ページビューは、従来ウェブサーバーからの配信回数を計測した値を採用していましたが、2007年3月からブラウザでの表示回数をCSCにより計測した値を採用しています。