画像ベースの本人認証によるフィッシング対策ソリューション

2008 年 8 月 15 日
株式会社ニーモニックセキュリティ

１．フィッシングの現状について

（1）フィシング対策技術取組みの具体的内容、方式説明効果を発揮する場面、および技術／製品名

フィッシングの脅威は更に深刻化することが確実視されており有効な対抗策が望まれるところですが、フィッシングへの対抗ばかりに気を取られて肝心の本人認証手段の確実性を損なうようなソリューションになってしまうことは避けなければなりません。

例えば、ワンタイムパスワード生成トークンが生成する乱数は使い捨てなので窃取に対して有効と考えられますが、もともとその一時乱数が証明しているのはそのトークンが真正であるということで、そのトークンを今保持しているのが正規の利用者なのか攻撃者であるのかについては何も語りません。つまり、本人認証の確実性という判断基準では、銀行カードさえ保持していれば暗証番号なしで預金を降ろせるというのと同じレベルのものであることに留意しておく必要があります。

（パスワードとの２要素で運用すると本人認証のセキュリティは向上しますが、そのパスワードが在来のものであれば本件の主題であるフィッシングなどによる窃取に対しては脆弱なことは周知の通りです。多くのユーザは同一のパスワードを多くのアカウントに使い回していることが知られており、そのような場合一つのアカウントでパスワードを窃取されると他の多くのアカウントが危険に曝されることになります。）

我々が提供しているような画像ベースの本人認証手段の運用方法に工夫を凝らしますと、利用者認証の確実性を維持しつつ本人認証情報の窃取を効果的に防止することができます。画像ベース本人認証の運用法の工夫によって対抗可能な本人認証情報の窃取攻撃には次のようなものがあります。

ａ）技術／製品名

一般名称：　画像ベース本人認証（長期記憶活用方式）
製品名称：　ニーモニックガード

ｂ）フィシング詐欺防御効果を発揮される場面

１）不特定多数を対象とする偽サーバによるフィッシング
２）特定個人を狙い撃ちする偽サーバによる標的型フィッシング
３）探知削除型の防御手段によっても捕捉されないトロイの木馬

ｃ）具体的方式／仕組み

１）不特定多数を対象とする偽サーバによるフィッシング

偽サーバによるフィッシング防御に以下の２つの方法を提供できます。
A-1:　認証画面をカスタマイズすることにより偽サーバの構築を困難にします。
A-2:　パスワードマネジャーを画像ベースの本人認証で管理運用し、破られにくい複数のパスワードを実際に運用することを可能にします。

２）特定個人を狙い撃ちする偽サーバによる標的型フィッシング

防御方法の骨子：　同一の認証画像をサーバと端末が共有しておき、正規のサーバと正規の端末および真正のユーザが揃った場合にのみ送信される情報が有意味で有用となる形で運用し偽サーバの存在の余地をなくします。

３）探知削除型の防御手段によっても捕捉されないトロイの木馬

防御方法の骨子：　トークンの真正性情報をワンタイム化するのではなく、本人認証情報そのものをワンタイム化しトロイの木馬を無力化します。

注：　中間者攻撃につきましてはこれらの方策だけでは対抗できません。他のベンダーから提供されている中間者攻撃対策ソリューションとの併用をお勧めしています。

（２）当該技術の特徴

先ず、ソリューションの基本となる長期記憶活用型の画像ベース本人認証技術の概要を説明します。

〖パニックとなる災害・危機現場でも使いこなせる本人認証技術〗

認証画面は３ｘ３～８ｘ８など自由に設定できます
写真以外にイラスト・漢字・英数字も使えます
暗証画像(パスシンボル)は「組み合わせ」も「順列」も登録できます
バックサイドで８０ビット（１０の２４乗）以上の文字列を運用できます

上の認証画面例にはペットの写真が１６枚並んでいます。この中から好きなものを適当に選んで覚えなさい、というのではありません。この中に昔自分になついていた犬の写真が何枚か含まれており、本人認証の必要な時にはこうした愛着のある犬を見つけてクリックするだけで強力なパスワードの入力と同じ効果を生み出す、というものです。新たに何かを覚える負担も、思い出そうとする負担もありません。

私達の人生体験の中に無限にあるこうした懐かしい想い出を伴ったイメージを使った暗証画像はいくら緊張していても慌てていても確実に認識することができます。パニック状況でも使えるという観点からは防衛省のセキュリティ幹部の認知を受け、子供にも使いこなせるという観点からはキッズデイザイン協議会から2008年度のキッズデザイン賞を受賞しています。

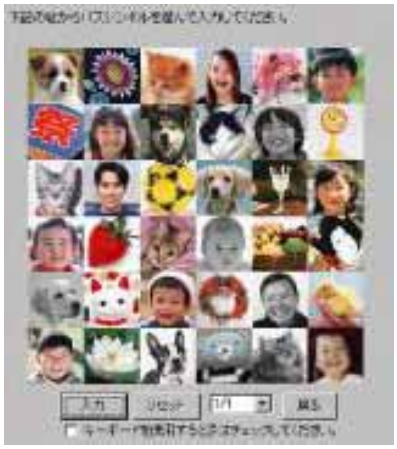
ユーザは自分が登録した愛着のある暗証画像を見つけ、過不足なく（組み合わせ方式）あるいは正しい順序で（順列方式）でクリックした上で入力ボタンを押します。本人でもやってしまうような間違いと本人ならやるはずのない間違いは区別してカウントする機能も使えます。肩越しの覗き見対策としては一時的に画像に割り当てられる文字列をキーボードからタイプ入力する機能や画像を１／２や１／４に縮小して表示する機能なども利用できます。

次に、フィシング対策として当社から提供できる４種類のソリューションについて、その概要を説明します。

A　不特定多数を対象とする偽サーバによるフィッシング対策

A-1:　認証画面のカスタマイズ運用

画像ベースの本人認証を導入すると、ログイン時のパスワード入力画面のところでユーザは次のような自分専用の認証画面を見ることになります。



偽サーバ排除のロジック

多数の認証画面を事前に用意するのは不可能ではないが費用対効果が著しく悪く、経済犯的なフィッシング犯は手を出せません。

アクセス毎に画像位置がランダムに変わると偽サーバ構築の経済コストは更に高くなります。

この偽サーバ排除機能は本人認証機能に内在されており、追加コストは発生しません。

オンライン決済システムで４年近い稼動実績があります。

A-2:　パスワードマネジャーを画像ベースの本人認証で管理運用

文字パスワードを画像ベース本人認証に変えてしまうという運用方式の導入が難しい場合には、現在使っている文字パスワードの脆弱性を補強する方法を提案します。

フィッシングによる被害を極小化するにはアカウント毎に異なるパスワードを使うことが望まれますがアカウントが多くなると記憶に頼るのは無理であり、パスワードマネジャーによるパスワード管理を望ましいソリューションとしてお勧めできます。

このパスワードマネジャーの利用者認証を慌てたり焦ったりすると思い出せない難解パスワードに任せるのではなくパニックでも使いこなせる懐かしい記憶を活用する画像ベースの本人認証で行うというものです。

画像ベース本人認証を通過すると画面右下のタスクトレイにアイコンが駐在し、右クリックすると表示されるメニューから「登録情報一覧」を選択すると登録済みのウェブサイトのリストが表示されます。目的のサイトをクリックするとＩＥが立ち上がり、目的のサイトにアクセスし、ＩＤ／パスワード入力ボックスにＩＤとパスワードを入力しログオンが完了します。ウェブサイトのみならずアプリケーションソフトにも対応します。

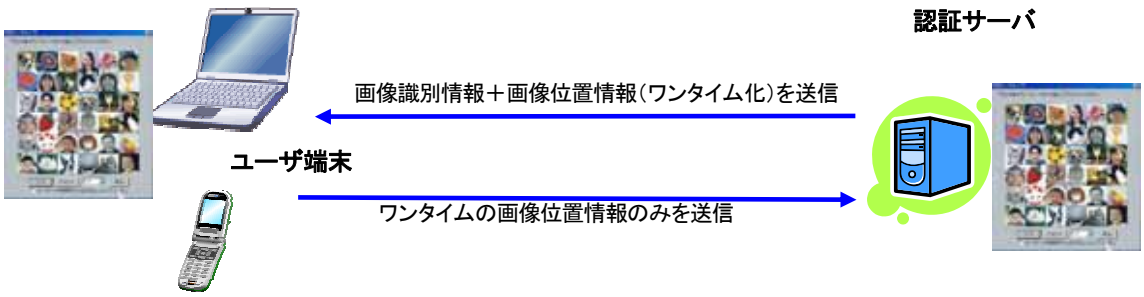
先にサイトにアクセスしている時にタスクロレイのアイコンをWクリックすると、そのサイトのＩＤ／パスワードを自動で探して入力を終えるという方法もあります。

ＵＳＢメモリーに搭載した汎用型製品として発売しています。

B　特定個人を狙い撃ちする偽サーバによる標的型フィッシング対策

運用方法とロジックは以下の通りです。

・サーバに保管されている認証画像のコピーを端末上にも保存します。アクセス毎に認証画面をサーバから端末に送ることはしません。認証開始時にはサーバから端末に画像識別情報と画像位置情報が流れるだけであり、ユーザが本人認証を実施した際には端末からサーバにユーザが選択した画像の位置情報が流れるだけです。



・アクセス時にはサーバ側で認証画像の位置を毎回ランダムにシャッフルし個々の画像に新たな位置情報を付与して画像識別情報とともに端末に送信します。

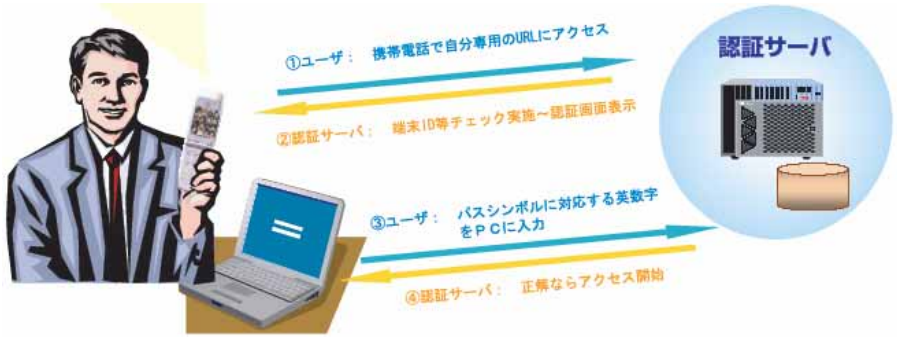
・ユーザ毎に組み合わせの異なる画像識別情報を正しく知らない攻撃者が構築する偽サーバは端末上の画像をシャッフル表示させる情報を送出できません。認証画像コピーの存在しない偽端末は画像シャッフル情報を受けても画像を表示することができません。

・正規端末上のみで本人認証を行うための画面を表示できます。また、正規サーバのみがユーザが選択した画像位置情報を意味のある情報として使用することができます。

このフィッシング偽サーバ排除機能は本人認証に何かを加えるものではなく、本人認証の運用方法の工夫によって実現できるもので、携帯電話で３年近くの運用の実績もあるものです。

C　探知削除型の防御手段に捕捉されないトロイの木馬対策

在来のいわゆるワンタイム製品が窃取を防いでいるのは『デバイス認証』情報ですが、画像ベースの本人認証手段を２経路２端末で運用すると『本人認証』情報のワンタイム化を実現できます。携帯電話に表示される認証画面を視認したユーザが自らの記憶からワンタイムパスワードを生成するのです。



携帯電話に表示される認証画像の一つ一つに異なる英数字がランダムに割り振られる →　パスシンボル（正解の暗証画像）は毎回異なる英数字列で表現される ＝　ＰＣから入力されるワンタイム英数字列はユーザの記憶を含む本人認証情報

在来の機械生成型の使い捨てパスワード製品は、使い捨て乱数を生成しているデバイス（トークンや携帯電話）が本物であることの証明はできますが、今そのデバイスを保持しているのが本人なのか或いは攻撃者であるのかについては何も語りません。本方式で使われる使い捨て乱数は、携帯電話の画面に表示されている画像群から暗証画像を正しく視認できる本人のみが生成できるもので、高い本人認証セキュリティを犠牲にせずに盗聴やトロイの木馬を無力化できる方式です。

携帯電話・ＰＣ共にブラウザーさえ搭載されていればよく、ユーザの作業も次のように簡単です。

１.事前に準備した認証画面を認証サーバに登録し携帯電話にアクセス用ＵＲＬを登録しておきます。

２．アクセス時には携帯電話からＵＲＬをクリックすると自分の認証画面と識別ＩＤを受信します。携帯電話に表示された認証画面上で暗証画像に割り振られている英数字列を認識し、その英数字列と識別ＩＤを認証サーバにアクセスしているＰＣ上で入力します。トロイの木馬が窃取した英数字列は使い捨てなので悪用できません。

（３）導入実績

Ａ：　オンライン決済システムで４年近い稼動実績があります。

Ｂ：　携帯電話利用によるオンライン決済システムで３年近い稼動実績があります。パスワードマネジャー複合製品はＵＳＢメモリー搭載商品として発売しています。

Ｃ：　導入実績は未だありませんが、長い運用実績のある１経路方式の入出力を２経路に改変するだけの簡単な作業で速やかに運用を始めることができます。

（４）今後の普及見通し

フィッシング対策の基本は本人認証の確実性にあるとの認識が広がるにつれて急速に普及するものと見込んでいます。

（５）課題

当社が零細な存在であることが普及の阻害要因となっていますので、産業界の信任の厚い有力企業から提案していただくことを追及します。

（６）開発の加速化方策

上記技術の根幹部分は産業総合研究所の情報セキュリティ研究センター所長をしておられる今井秀樹クリプトレック座長が東京大学生産技術研究所におられたころに共同研究事業の中で開発したものです。今後も今井秀樹東大名誉教授のチームとの連携を図りながら開発を加速化する計画です。

２．携帯電話端末向け技術の取組みの有無、重要となる技術、市場の見通し

当社の本人認証窃取防止技術は、PC であれ携帯電話であれ、どのような端末でも利用可能です。一方ではフラッシュなど機種依存の少ない技術が与件として存在し、他方ではｉＰｈｏｎｅやＡｎｄｒｏｉｄなどオープンなプラットフォームの普及拡大が予測されています。またＰｉｃａｓａのような無償の画像収集・編集ソフトの普及によって当社技術普及にとって更に好ましい環境が現出しています。当社技術がお役に立てる分野は更に広まるものと考えています。

３．フィッシング対策の展望

本人認証情報を窃取しえた攻撃者はその本人認証情報の持ち主がアクセスできる情報資産の全てを自由にできるのですから、ネット上での資産の蓄積が進む限りあらゆる手段を駆使した攻撃を無制限に続けるものと考えておく必要があります。当社では先述の今井チームと連携して本人認証専用の携帯デバイスを開発する構想を抱いています。これは目前にある端末が攻撃者の支配下にある可能性を否定できない状況であっても本人認証情報の窃取を防ぎつつその端末を利用可能としようとするものです。技術上の課題は克服できるものであり、こうしたデバイスを必要とする産業界の意思が固まれば世界に先駆けて実現することができます。

４．その他

新しい脅威に気を取られるあまりに古い脅威に対する警戒心が薄れてしまうと攻撃者の思う壺にはまってしまいます。新たなフィッシング手法の登場は古典的な本人認証情報窃取の脅威の軽減を意味するものではありません。攻撃側は大昔にもあった犯罪手法から最新の手法まで自由に選択でき自由に組み合わせることができるのですから。

この観点からはノートＰＣ・携帯電話・スマートフォンなどによるモバイルコンピューティングの普及は攻撃側にとっては攻撃手法の選択肢を大きく広げるもので、我々防衛側にとっては更に難しい課題の解決を迫られることになります。モバイル環境ではハッキングやソーシアルエンジニアリングなどのハイテク型ないしインテリ型の攻撃に加え置き引きや強奪さらには脅迫など太古の昔から存在した攻撃手法まで全方位での防御を考えなければなりません。

伝統的犯罪手法からハイテク型攻撃手法まで全ての可能性を念頭におきつつ、（１）モバイル環境でパニック状態になっても使いこなせる本人認証手段の確実性を維持しながら（２）同時にその本人認証情報の窃取対策を図ることが必要です。（１）だけでも駄目、（２）だけでも駄目、（１）と（２）を二つながらに達成することが必要です。当社ではそのような包括的ソリューションを提供し続けるべく鋭意努力を続けます。