インターネットでの不正行為 その傾向と対策

すべての不正行為を防ぐのは不可能です。しかし、防ぐためのテクノロジーは日々進歩を遂げています。今回は、そんな将来の技術について取り上げます。最新技術の情報を集めて知識を得ておくのも、不正行為の被害を受けないための重要なことです。

第9回 これから求められる技術

JPCERT/CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

今日から明日へ

今回、お話しするのはワンタイムパスワードとSSHです。ただし、本稿を執筆している時点（1998年春）では、一般に広まっている技術とは言い難いものです。また、将来は、ワンタイムパスワードやSSHのようなシステムが一般に広がるでしょうが、現在使用しているようなソフトウェアや製品がそのまま使われるかどうかはわかりません。しかし、「明日の技術」をお話しすることはより広い知識を身につけるための一歩になると考え、今回のテーマとしました。

よく、世間で散見される不正アクセスに関する説明の中に「現在は、（今回説明する範囲のような）いくつかの不正アクセスに対する技術がない」という、少し誤解を招くような表現があります。しかし、これは正確ではありません。

正しくは、「不正アクセスに対応する技術の導入が一般には進んでいない」、あるいは「不正アクセスに対応する技術に関して認知が不足している」というべきでしょう。

今回のテーマは必ずしも特殊な話題とは考えていません。紹介する技術は、確かに一般には広がっていませんが、すでに一部では日常的に使われている技術です。それは、ちょうど10年前のインターネットに似ています。

インターネットは10年前でも一部の人の間では日常的に使われていたのですが、一般に広がるまでには、その後、数年を要しました。その時と同じように、今回お話しする内容も、近い将来、広く使われる技術となることでしょう。たとえ、現在と同じ形ではなくとも、ベースとなる技術でしょう。

パスワードの問題点

現在、主流として使われているパスワードの概念や問題点は、連載第3回の“パスワードについて心がけてほしいこと”[1]で解説しました。ここでは、パスワードの問題点が何か

[*1] 過去のバックナンバー
URL http://www.jpcert.or.jp/magazine/beginners.html

をもう一度確認してみたいと思います。

パスワードが類推される

利用者が入力するタイプのパスワードは、基本的に人間の記憶に頼ります。したがって、多くの利用者は簡単に思い出せるパスワードにする傾向があります。もし、利用者が弱いパスワードを選択してしまうと、一定条件の下では数分から数時間の間でパスワードが類推されてしまう恐れがあります。

たとえ、利用者に弱いパスワードではいけないということを徹底して教育しても、あるいは、運用規則として取り入れても、完全にすべての利用者が“弱いパスワード”を使わなくなるという保証はありません。また、管理者やセキュリティー担当者がパスワード選択に関与するということも現在の記憶に頼るタイプのパスワードでは難しい問題でしょう。

ネットワークが盗聴される

どんなに安全なパスワードを使用していても、ネットワーク上で盗聴が行われればパスワードは筒抜けです。ほとんどのネットワーク上の盗聴は、ローカルネットワークの弱点を突く形で行われます。ローカルネットワーク敷設時に、盗聴の難しい設計を行い、その後の運用も的確な方法で行っていれば、ネットワーク盗聴が困難となります。そうすれば、危険性は格段に少なくなるでしょう。しかし、既存の多くのローカルネットワークではネットワーク盗聴を想定して設計されていません。

また、ネットワーク盗聴を難しくするローカルネットワークを作る費用は、何も行わないものよりもコストが上昇する傾向があります。そのため、これから敷設するローカルネットワークが必ずしも盗聴に対応できるようなネットワークだとは限らないでしょう。

広域なネットワークを利用するすべての場合に当てはまることですが、自分の発信したデータが相手に着信するまでのあいだ、どのようなネットワークを経由するかを確実に把握するのは、ネットワークの規模が大きくなればなるほど難しくなります。そして、経由するネットワークすべてが安全なネットワークであるかどうかの状況を把握することはさらに困難を伴います。いくつも通過するであろうネットワークのどれか1つに安全ではないネットワークが入ってしまえば、安全性の欠けるネットワークとなります。

ワンタイムパスワード

通常のパスワードによる認証は、事前に登録しておいたパスワードと同じパスワードであるかを比較する方法です。新しいパスワードに変更しない限り、毎回、同じパスワードを入力します。

ワンタイムパスワードも、通常のパスワードとは異なり、システムに接続するなどの認証に使うパスワードは、毎回違うパスワードにできます。つまり、一度しか（あるいはごく限られた期間や回数のみ）しか有効ではありません。

パスワード類推によるアタックは、事前に登録しておいたパスワードを見つけ出すために試行を繰り返す方法です。ワンタイムパスワードは一度しかチャンスがないので、パスワード類推によるアタックが非常に困難になります。

ワンタイムパスワードには、大きく分類して2種類あります。1つは、チャレンジレスポンスと呼ばれる、外部から補助パラメータを与える方法です。もう1つは、内部のデータのみから自動的にワンタイムパスワードを生成する方法です。

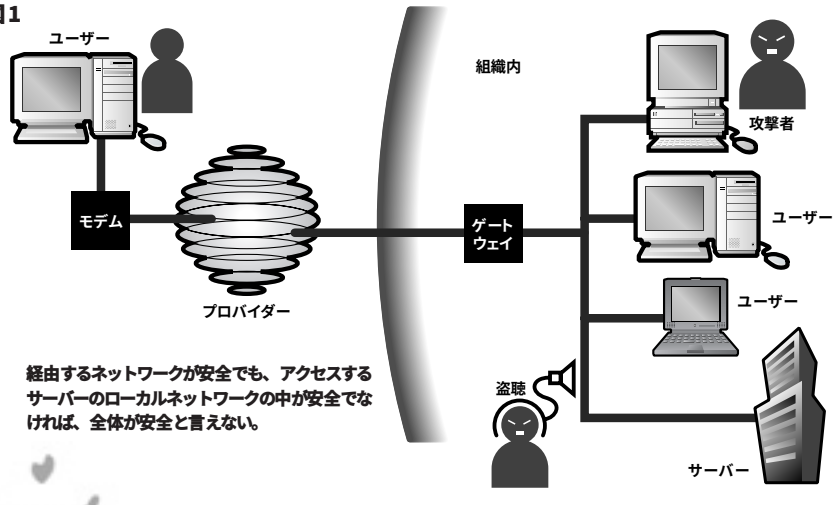
生成の原理

本稿では、チャレンジレスポンス方式に分類される単純なワンタイムパスワードのモデルを説明しましょう。説明中は、認証を行なう側をサーバー、使用者側をクライアントとしています。

最初に“種”となる初期値を用意します。これは、サーバーとクライアントの両方が所有します。この“種”が有効である認証の回数を9回とします。

❶クライアントがワンタイムパスワードを生成するために、サーバーにチャレンジレスポンスの値を要求する。
❷サーバーがチャレンジレスポンスの値をクライアントに送る。初めての認証ならば10の値を渡す。N回目の認証ならば、10－Nの値を渡す。
❸クライアントは、サーバーのチャレンジレスポンスの値である回数分、“種”を一方向性ハッシュ関数に繰り返しかけ、その値をワンタイムパスワードとする。

図1



❹サーバーも同じく、チャレンジレスポンスの値と“種”を使ってワンタイムパスワードを計算する。

❺クライアントは、ワンタイムパスワードの値をサーバーに送る。サーバーは、自分で計算したワンタイムパスワードの値と比較する。同じ値ならば、正しい（ワンタイム）パスワードであると認める。

この単純なモデルのポイントは、“種”に対し一方向性ハッシュ関数で処理を必要回数分繰り返す部分と、その必要回数が必ず少なくなっていくということです。説明では9回としていますが、9回の認証を行うと、この“種”の寿命はつきてしまい、また初期値をサーバーとクライアントの両方に登録しなおさなければなりません。

一方向性ハッシュ関数を補足すると、「一方向性」という言葉が示すように出力から入力には戻すことができない関数です。さらに「わずかな入力の違いで、出力に大きな違いが発生する」「入力のデータサイズにかかわらず、出力されるデータサイズは一定」「異なる入力に対し出力が同じであることは極めてまれである」というような関数です。一方向性ハッシュ関数として有名なアルゴリズムにMD5やSHA-1などがあります。

さて、一方向性ハッシュ関数で繰り返し処理する回数を毎回少なくするという利点はどこにあるのでしょうか。それは、すでに使用されたワンタイムパスワードを知られていても、次回に発生させるワンタイムパスワードは分からないという点です。

ここでは説明を分かりやすくするために、9回としていますが、通常のシステムでは、もっと繰り返し使えるような大きな値になっています。

ワンタイムパスワードのクライアントは、ポケット電卓のように専用のハードウェアになっているもの、あるいはアプリケーションとして実現されているものなどがあります。ハードウェアで実現されているものは“種”の値がハードウェア内に格納されており、それは外部からアクセスできないような構造になっています。アプリケーションで実現されているものは、“種”を通常のパスワードと同様な方法で入力します。ただし、そのユーザーが入力したパスワードはアプリケーション内のみで使用され、ネットワーク上には現れません。

SSHとは

UNIXには、ネットワークで接続されたマシンに対して、ログインするrlogin、コマンドを実行するrsh、そしてファイルをコピーするrshなどのコマンドが用意されています。そのコマンドに代り、暗号技術を導入してサーバーとクライアント間で安全に通信を行うために、認証と暗号化を行なうのが、SSH（Secure SHell）です。SSHは、その他にもX-Windowで使用するプロトコルに対して同様の暗号技術を用いて安全な接続も可能にします。サーバーはUNIXですが、Windows95、Macintosh、OS/2で動作するクライアントが存在しています。

SSHの防御範囲

SSHは暗号技術によって次のような攻撃を無効にします。

●エアパケット偽造などの
攻撃に対する対抗策

暗号技術を使って認証を行うので、サーバーやクライアントが偽造したIPアドレスを使う攻撃を仕掛けても、SSHを用いることによって攻撃を無効にします。また、DNSに関しても同様です。

「ネットワークを介して接続した先は、実は偽造されたサーバーだった」、あるいは、「IPアドレスによってクライアントをフィルタリングしているようなシステムに対し、クライアントから偽造したIPアドレスを使用してアクセスされた」というようなことが発生する可能性があります。IPアドレスには関係なく、SSH自身によって認証を行えば、IPアドレス

図2：一方向性ハッシュ関数のモデル

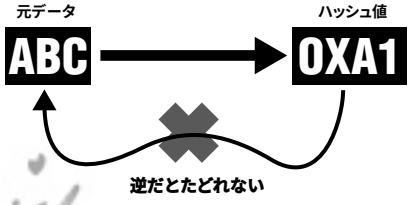
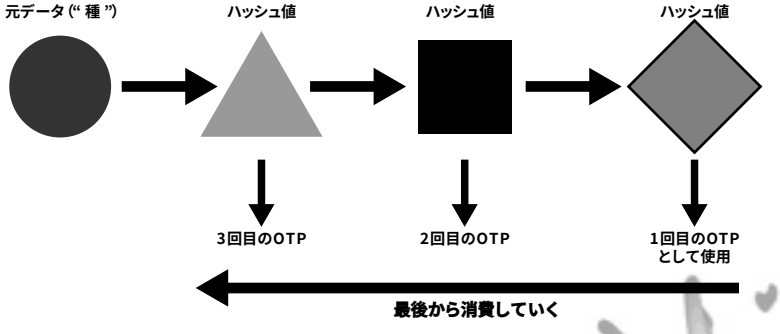


図3：3回分のワンタイムパスワード（OTP）のモデル



偽造による攻撃は無効になります（ただし、SSHがカバーするrlogin、rsh、rcp、あるいはX-windowに対する攻撃のみ）。

●ネットワーク盗聴などに対する対抗策

サーバーとクライアントの間は暗号化したデータでやり取りするので、ネットワーク盗聴ができなくなります。同じ理由で、途中でのデータの改竄、あるいは、サーバーとクライアントの間で行っているネットワークの通信の乗っ取りもできなくなります。

たとえば、ネットワークを介してログインし、ROOT（管理者の権限）としてシステムのメンテナンス作業を行うようなとき、もしネットワーク盗聴が行われていていたならば、ROOTのパスワードも含めて重要な情報が筒抜けになってしまいます。SSHでは、そのような危険性がなくなります。

使用される暗号技術

サーバーとクライアントの間で通常の通信に使用される暗号は、十分に安全である共通鍵暗号法が用いられています。現在は、共通鍵暗号法のアルゴリズムとしてIDEAやTriple DES などが用いられています。

暗号通信を開始するときに行われる共通鍵暗号のための鍵交換は、公開鍵暗号法を用いて行われます。また、共通鍵暗号に使う鍵は使い捨てになっています。現在は、公開鍵暗号法のアルゴリズムとしてRSA法が用いられています。

認証には、電子署名の技術が用いられます。現在は、電子署名のアルゴリズムとしてRSA法が用いられています。使用されている具体的なアルゴリズムも、今後、さらに安全なもの、あるいは高速なものが使われることでしょう。

SSHの動作概要

ここでは、サーバーへログインすることを説明に使いましょう。

事前に、サーバーとクライアントは、お互いに公開鍵を交換しておきます。相手の公開鍵が正しいかどうかの説明はここでは省略して、正しい相手の公開鍵を交換できていることにします。

❶サーバーとクライアントの間で毎回のログインを開始するときに、その都度、新たな電子署名によって署名したデータを用意して交換します。その署名が正しいか否かを各々チェックします。署名が正しければ正しい相手です。この電子署名のチェックには、すでに交換してある相手の公開鍵が用いられます。

ここで、認証（電子署名のチェック）はSSH自身が行うので、IPアドレスが偽造されているといったことに左右されずに相手をチェックできます。

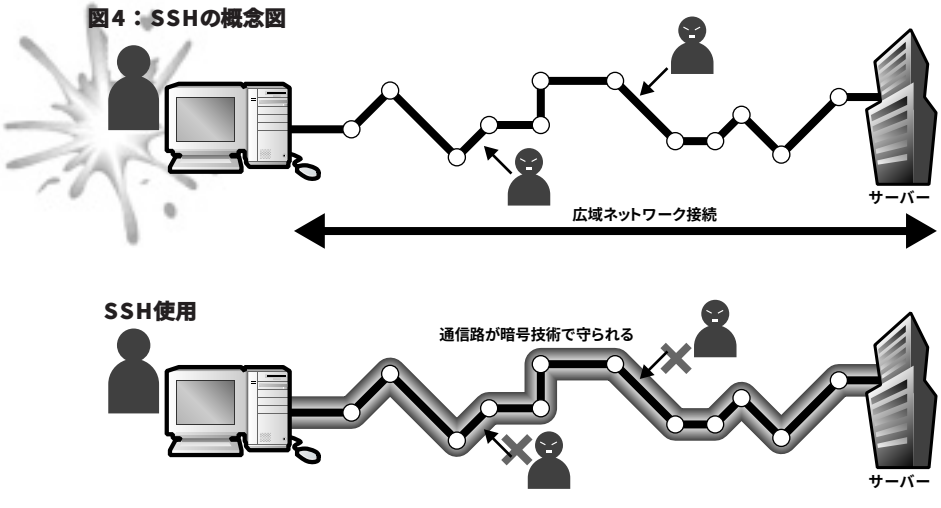
❷公開鍵暗号法を用いて、通信のときに使用する暗号の秘密鍵を交換します。

❸交換した秘密鍵を用いて、共通鍵暗号で暗号化したデータのやり取りを開始します。

共通鍵暗号は高速に暗号化／復号化ができるので、通常の通信は共通鍵暗号を用いて暗号化を行なっています。

通信でやり取りしているデータが暗号化がされていれば、たとえ、ネットワークを盗聴したとしても、中身が守られています。

図4：SSHの概念図



さらに将来は

IPv6という次世代IPの仕様では、IPのパケット自体にSSHのような暗号技術が取り入れられます。IPv6が普及すると、新たに特別なシステムやアプリケーションを導入しなくとも、安全にネットワーク上で通信ができるようになるでしょう。

まとめ

今まで防御が難しいと言われてきたいくつかの不正アクセスに対し根本的にシャットアウトできる可能性をもつ技術がすでに存在しています。その問題点は、一部にしか普及していない技術であるということです。

今回は、あまり一般には知られていない技術を短い文章で紹介しているため、分かりづらい部分もあったかと思います。しかし、必ずしも技術的な部分の理解が必須ではありません。「現在知られている既存の不正アクセスに関しては、多くの問題に対して対抗策が存在している」という感想を持って頂ければ、十分に本稿の目的は達したことになるのです。

本連載に対するご意見やご質問、不正アクセスに関して知りたいことがありましたら以下のメールアドレスまで。今後の参考にさせていただきます。

E-mail ip-security@impress.co.jp

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp