2002-9-15

H．P．Report

第56号

発行責任者　稲崎義明

セキュリティと暗号（１３）

暗号の解読には、解読者に都合のいい条件がついています。確かに、それだけ都合のいい条件がついてもなかなか解読できないのですから、問題ないのですが、はたしてそうでしょうか。共通鍵暗号を使った場合、相手がこの暗号を使って送っていいかどうかを判断するために認証しますが、実際は次のように相手を認証します。

通信相手が正等であるかどうかを確認しようとするユーザＡが、通信相手のユーザＢに対して、秘密情報である鍵データを直接送信することなく、秘密情報を知っているという事実だけを納得させることで、相互に相手を確認しようとする方法です。もちろんこの場合、同じ暗号のアルゴリズムと鍵データを持っているものとします。まず、ユーザＡはユーザＢに対して任意の平文を送信します。受信したユーザＢはこの平文データを自分の持っている鍵データで暗号化し、その暗号データをユーザＡに送り返します。受け取ったユーザＡはもともとの平文データを自分の持つ鍵データで暗号化し、このデータとユーザＢから受信したデータを比較し、合っていればユーザＢを正当な相手として確認することができます。このときユーザＡは認証を行うごとに平分を変えて送り相手を確認しなければなりません。同じデータを二度使うと、前回の通信を盗聴していた解読者が、前回ユーザＢが送り返した暗号化されたデータをユーザＢより早く送り返すことによってなりすますことができます。

この認証方式の場合、解読者は1度の認証行為によって平文と暗号文のペアを入手することができます。つまり、高性能な線形分析法による解読でも平文と暗号文のデータを2^{43}組必要と書きましたが、この数字あまりにも都合のいい数字とはいえなくなります。通信の盗聴を続けていることによって、認証しようとするたびに、違った平文データと暗号化されたデータを入手することができるわけですから、時間を掛さえすれば、大量の平文、暗号文のペアデータを入手でき、既知平文攻撃の環境が成立することになります。もっと条件のいい選択平文攻撃のためのデータを収集しようとする場合には、ユーザＡになりすまし、ユーザＢに対して自分で自由に作った平文を認証行為のようになりすまして送れば、ユーザＢは送った平文に対する暗号文を自由に入手することができることになります。なりすますことさえできれば、暗号解読のために条件のよりよい選択平文攻撃のためのデータを入手することができるわけです。

実際の線形解読法による暗号解読では、ＤＥＳの場合であれば56ビットの鍵データのすべてをこの解読法で解読するわけではなく、1段から16段まである暗号処理のうち、2段目から15段目までの変換を1つの関数とみなして解析することによって、６ビット＋６ビット＋１の13ビットと、平文と暗号文を入れ替えることによって得られる13ビットの合わせて26ビットを特定し、残り30ビットについては総当り方式で求められました。このように、線形解読法といえども、効率をはかるために複数の方法を組み合わせて実際の解読は行われています。

ＤＥＳは20年解読されませんでした。しかし、暗号の安全性を定量的に表現できれば、この暗号はあの暗号よりも安全という判断ができます。この暗号は大丈夫ですといっても簡単に解読されるものかどうかが分からなければ納得できません。それが差分解読法に対する「差分特性確率」や「平均差分確率」であり、線形解読法に対する「線形特性確立」や「平均線形確率」です。この値が十分に小さければ、数学的にこの暗号は安全と証明することができます。（次回へ続く）

(情報誌トピックス)

○日経エレクトロニクス　９月９日号

特集　中国の技術者、世界へ

→シリコンバレーから中国へ。シリコンバレーで経験、技術を吸収した技術者が優秀かつ勤勉、低賃金でよく働く中国(上海)に戻り起業している。日本人技術者の強力なライバルになるのは目の前。

解説　アンテナで乗り切るＡＶ家電の無線化

→家庭でＨＤＴＶ並の高画質映像を、家庭内の機器間で途切れることなく無線伝送するには、実効スループットは23Mビット／秒を達成し、伝送距離は30ｍを確保する必要がある。もうここまでくれば無線回路のチップセットやアナログ回路部品の性能向上では追いつかない。そこでＰＨＳに採用されたアダプティブアレーアンテナなどに注目が集まっている。

○日経パソコン　９月１６日号

特集　パソコン「遅さ」の研究

→起動や終了、アプリケーションの動作など最新マシンであっても「遅い」と感じることはある。避けられないものもある一方でテクニックによって対処できる遅さもある。

特集　３００万画素小型デジカメ

→標準的となった３００万画素のデジカメで、マニュアル露出、露出補正、スポット露出、マクロ撮影など、カメラ好きが使えるカメラを選ぶ

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　１０月１日号

特集　拡張パーツ買い得指南

→限られた予算の中で効率よいパワーアップをするにはどうすればよいか。ＰｅｎｔｉｕｍⅢ(Ａｔｈｌｏｎ)をベースに予算５０００円から６万円までのグレードアップの指南。

特集　マルチディスプレイ操縦法

→ＡＴＩテクノロジーのＲＡＤＥＯＮ９７００を使った高性能ビデオボードによるグラフィック性能と、マルチディスプレイの使い方の紹介。

特集　１２Ｍｂｐｓ　ＡＤＳＬの真実

→Ｙａｈｏｏ！ＢＢの始めた１２ＭｂｐｓのＡＤＳＬサービス。いろいろ問題も発生しているようだが、実際のメリットは、高速化よりも４ｋｍから７ｋｍに伸びた利用可能距離にある。