2002-9-1

H. P. Report

第55号

発行責任者 稲崎義明

セキュリティと暗号（１２）

線形解読法についてですが、前にも書きましたとおり、この解読法はブロック暗号のための解読法です。ＤＥＳもブロック解読法ですが、これは、平文をブロックと呼ばれる一定の長さのデータに分割して、そのブロックごとに暗号化する方法です。多くのブロック暗号のアルゴリズムは、１ブロックを８バイトとすることが多く、また、共通鍵方式に属しています。

ブロック暗号の処理は、鍵スケジュール部とデータランダム化処理部の二つからなります。鍵スケジュール部は、鍵データを演算処理することによりデータランダム化処理部にその結果をデータとして供給します。1つの鍵データから複数の鍵データを演算処理により生成するわけですから、鍵スケジュール部で生成されたデータを、拡大鍵データといいます。データランダム化処理部は、平文データを暗号文データに変換する処理を行います。処理としては、平文データと鍵スケジュール部で作られた拡大鍵の排他的論理和や、置換と呼ばれるデータ変換を組み合わせた操作を複数回繰り返します。1回の繰り返しを1段の処理というように繰り返し回数を段数と呼びます。ＤＥＳの場合は16段ですから、操作が16回繰り返されることになります。一般に段数が増えることによって暗号化処理は複雑になりますから、解読に対する強度は高まることになりますが、段数を増すことによって処理に時間がかかることになります。暗号強度と処理時間のバランスをとることが必要になります。

線形解読法は、暗号化の変換処理の一部をより簡単な関数で近似し、その結果得られた変換処理を用いて鍵データを推定する方法です。このことによって鍵データを求める計算量を減らすことができます。この変換処理を近似する方法として、線形近似を用いているため、線形解読法と呼びます。この手法は、平文データと暗号文データのわずかな相関を手がかりにします。理想的にランダムな暗号の場合、入力データと出力データに相関はないのですが、実際の暗号の場合には、この相関が少なからず存在しています。具体的な解読の手順としては、暗号化の第1段から第r－1段までを簡単のため関数Ｔとします。解読する際に入力データと出力データの関係を調べて、平文のある1ビットと、関数Ｔの出力(第ｒ段入力となる)のある1ビットが一致する理論上の確率P_1を求めます。その確率P_1が1／2から離れていればこの二つのビットに相関があったということで、関数Ｔの変換処理に偏りがあったということになり、鍵データを推定できる可能性が出てきます。つまり、解読する際にｒ段目に使う拡大鍵データK_rの候補1つについて、与えられた暗号文データから第ｒ段の入力データを逆算します。このような作業を用意した多数の平文データと暗号文データの組を使って繰り返すことによって、ｒ－1段の出力の指定したビットが平文データの指定したビットと一致する確立P_2を求めます。この作業を鍵データの候補すべてに対して行います。鍵データが間違っていれば確率P_2は1／2に近くなり、正しい場合は確率P_2は確率P_1に近い値をとると考えられます。こうして鍵データの一部を特定することができます。残りの鍵データは候補を全部調べる方法で探すのですが、それでも鍵データの全ビットの候補を探索するよりも計算量を少なくすることができます。この他、線形解読法では、できるだけ相関の強いビットを選んで解読することによってできるだけ少ない計算量で解読することができます。また、平文データのあるビットが多くの場合“０”になり、そのことを解読者が知っていると仮定すれば、暗号文データだけで解読することも可能となります。

（次回へ続く）

(情報誌トピックス)

○日経エレクトロニクス　８月２６日号
　特集　「０５０」を旗印に、電話国盗り合戦
　　→この秋ＩＰ電話に「０５０」のＩＰ電話専用の番号が登場する。ＩＰ電話で誰もが電話会社になることができるようになる。これまでの電話会社は、認証、課金、ネットワーク、端末といった各要素をまとめて提供してきた「垂直統合型ビジネス」であった。ＩＰ電話では、各要素をそれぞれの分野で強みを持つ企業が担当する「水平分業型ビジネス」へと転換する。しかし、現実は接続性と品質評価で混乱している。
　解説　近距離無線をケータイが牽引　ＩｒＤＡを先頭に一気に市場に
　　→携帯電話、ＰＤＡ、白物家電、おもちゃ、センサーなど、多様な機器に近距離無線が搭載される。どこもが最新ケータイに搭載したことで、自動販売機やレストランなどでの利用から市場が形成されている。

○日経パソコン　９月２日号
　特集　気になる愛器のプライバシー
　　→手になじんだ万年筆とパソコンは他人に貸さないほうがいい。パソコンからはいろいろな情報が取り出せる。ファイルやメールが見られるだけでなく、インターネットの履歴やファイルから最近の仕事まで分かる。貸す、借りる、共用するなどのパソコンを使う上での知友移転と対策を特集。
　特集　基礎から学ぶアップデート
　　→提供されているアプリケーションは、定期的にアップデートが必要になる。特にマイクロソフトの製品は、セキュリティ対策のためにも必要となる。ではどのようにアップデートすればよいのか。ＢＩＯＳからＯＳ、アプリケーションに分けてその基礎から整理する。

○日経バイト　９月号
　特集　電磁波影響の研究
　　→携帯電話からの電磁波、テレビからに始まり、電気が流れていれば電磁波は発生する。では、電磁波とは何かから、機器への電磁波障害と人体への影響までを探る。
　特集　ＮＡＴの限界
　　→ＮＡＴ(NetworkAddressTranslator)は、１つのグローバルアドレスを複数の端末で共有することのできる技術である。しかし、IP電話などでインターネットを通して端末同士で通信するＰ２Ｐ(Peer-to-Peer)型のアプリケーションが増えＮＡＴの存在が問題視されてきた。Ｐ２Ｐのアプリケーションについて、その現状と回避策を探る。
　ﾚﾎﾟｰﾄ　Ｗｉｎｄｏｗｓに潜むデフォルト設定の落とし穴
　　→Ｗｉｎｄｏｗｓをデフォルト設定で使うと複数のポートがオープンしたり、自動で複数のサービスが起動したりしている。便利な面もあるが、外からの攻撃の格好のターゲットとなる。きちんと見極めて、適正な設定をするには。

○日経オープンシステム　９月号
　特集　後で苦労しないアプリケーション開発

→「短期開発」「頻繁な仕様変更」によって後で苦労するシステムが多いが、いろいろな手法を、駆使し正しい使い方をすることによって、後で苦労しないシステムを構築するには。

○N＋I　NETWORK Guide　9月号
特集　ファイアウォールを今、見直せ！！
→日ごとに高まるセキュリティの脅威に対抗するため、高機能化しようとしているファイアウォールをどのように使えばいいのか。自社システムのセキュリティとシステムのために、ファイアウォールをどう選び、どう設定すればいいのか。
特集　ログ･分析と対処の実践マニュアル
→攻撃の前兆を見抜き、不正侵入をどう防ぐのか。ログで分かる不正侵入の分析と対策。ホスト監視型ＩＤＥの「ＢｌａｃｋＩＣＥ」の活用について。

○ＡＳＣＩＩ　9月号
特集　最強録画ＰＣ化計画
→家庭用ＰＣで動画を取り扱うことができるようになってきた。書き込み型ＤＶＤを使ったり、ネットで流通し始めた動画ファイルを利用したり。自分のＰＣを最強の動画対応ＰＣにするには。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　9月１５日号
特集　極楽マザー１８０選
→完成品のＰＣが値下がりし、自作ＰＣへの関心度も今一歩というところの感じがする(私だけかな)が、マザーボードもいろいろなものが短い周期で発売されている。最新のチップセットの評価と各種インターフェースを中心に、国内発売のほぼ全種類のマザーボードカタログを掲載。
特集　動画圧縮の神業
→ＤＶＤレコーダが認知され、普及が始まっているが、専用のＤＶＤレコーダ以上のことがＰＣで実現できないか、そのノウハウの紹介。ビデオキャプチャーによる高画質録画から、ＰＣならでは使い方にはどういったものがあるか。