ネットワーク構成運用論

芸術情報設計学科
2004/06/21
藤村直美

セキュリティ（個人）

- 認証技術（アカウントとパスワード）
- 電子メールの暗号化 (PEM, PGP)
- SSH、SSL
- ウイルス
- ファイヤーウオール
- パケットフィルターリング

ＰＥＭ（Privacy Enhanced Mail）

- RFC1421～RFC1424（メッセージ（メール）の暗号・復号化のための規格）
- メールの本文を暗号化し、デジタル署名を付けて本文を送信
- 本文の暗号化にはDES-CBCを、デジタル署名にはRSAを使用
- PEMでは階層的な認証システムを使っており、どこか1カ所にある信頼できる機関に公開キーを登録しておき、それを使うことによって通信相手を認証

PGP

- Philip Zimmermann氏が開発した暗号化ソフトとその規格
- 1991年にWebで公開され、世界中に普及
- 電子メールやファイルの暗号化に用いられ、ほとんどのプラットフォームで利用可能
- 公開鍵暗号アルゴリズムを用いて、メッセージの暗号化
- 送り手の同一性とメッセージの改竄を防ぐための電子認証の機能を有する

PGP(2)

- インターネット標準としてのメッセージ交換方式、RFC1991（バージョン2.x）、RFC2440（OpenPGP）
- PGPは開発当初は米国の暗号化輸出規制の対象で輸出禁止だった（印刷したソースに基づいた「国際版」が併存）
- 1999年12月に米国の輸出規制が解かれ、Network Associates(NAI)が輸出許可を得た
- 国内のフリー＆シェアウェアのメーラの多くが外部プログラムとしてPGPをサポート

SSL,SSH

- インターネット上では特にデータは暗号化されていない→誰でも盗聴可能
- ホスト間で認証して、通信を暗号化する→誰でも盗聴ができるわけではなくなる
- SSHでは
  - RSA認証に公開鍵暗号を使用している
  - サーバから共通鍵を公開鍵の仕組みを使って送る
- SSLでは
  - PKIが機能している

ウイルスとは

- 一般的に次の行動パターンを持つ不正プログラムをウイルス
  - **感染**
    他のファイルにウイルス自身を付着させる
  - **潜伏**
    一定の条件が揃うのを待って悪質な行動をする
  - **発病**
    データの破壊、動作の不安定などユーザの意図しない行動をする
- 本来のウイルスの定義からははずれるが、他のプログラムに感染（寄生）する習性を持たず、プログラム自身がユーザの意図しない行動をする不正プログラムを「ワーム」「トロイの木馬」などと呼ぶ

http://www.trendmicro.com/jp/security/general/what/overview.htm

ウイルスの感染経路

- メールの交換
- インターネット上からのファイルをダウンロード
- 他のコンピュータとのデータを共有
- フロッピーディスク、MO、CDなどでデータを交換
- パソコンを持ち出して感染する

ウイルスの被害

- メールを勝手に送信（ファイルを添付する）
- ハードディスク内のデータを破壊
- 外部からコンピュータを操作可能にする
- システムを不安定にする
- 余計なメッセージを表示する
- 他

セキュリティ（組織）

- オープンな接続
  望ましいが危ない
- 部分的に制限した接続
  ゲートウェイでパケットを制御
- ファイアウオールを介した接続
  できるだけ自由に、しかし規制も
- 組織ネットワークと隔離した接続
  本当に危ないデータを守る場合など

外部からの攻撃

- 直接接続するもの
  - Code Red（2001年7月）、NIMDA（2001年9月）
- メールを媒体にするもの
  - SIRCAM、MTX
- WWWのアクセスによるもの
  - 怪しいHP

不正アクセス

- セキュリティホール、ポートスキャン攻撃
- パスワードファイルの入手と解読
- 不法ログイン
  - ファイルの削除、改変
  - 他人に成りすまし→他組織を攻撃
- SPAMメール、サービス不能攻撃

IDS

- Intruder Detecting System
- 外部からの攻撃を検出する専用装置
- ホスト型／ネットワーク型
- 攻撃パターンを手動で設定するものと自動で設定するもの
- 攻撃パターンを学習するもの
- ログが大量にでる→なかなか見ない
- 回線速度が速いとつらくなる

ファイアウオール

- インターネットと内部の間で
  - 外部から内部への不正なアクセスを防止、
  - 不正なデータが内部から外部へ送信される

  ことを防ぐソフトまたはハード
- 機能としては
  - パケットフィルタリング
  - アプリケーションレベルゲートウェイ
  - ロギング

ファイアウオールの限界

- ファイアウオールの外に置くサーバに対する攻撃は防げない
- ファイアウオール内でも外部にサービスを提供するサーバはセキュリティホールをついた攻撃を受ける
- メールによるウイルス
- CGIによる不正アクセス
- 各種の設定ミス

パケットフィルタリング

- IPパケットのヘッダーを監視して許可･不許可を判断
  - 送信元、受信先IPアドレス
  - TCP/UDPヘッダーの送信／受信ポート番号→アプリケーションがわかる
  - 送信の方向（外向け／内向け）
    - TCPの接続要求に対する応答ではTCPヘッダーのACKがon
    - UDPでは送信元がポート番号を記憶している

ファイアウォール

- ルータの一種
- 組織の内部と外部で不必要な通信を切断
- 芸工大では
  - 1996年1月　3ポート
  - 1996年8月　6ポート
  - 2001年2月　36ポート
  - 2002年2月　原則閉鎖

ftpとファイアウオール

- ftpは21番（制御）と20番（データ）の2ポートを使用してTCP通信を実施
- 外部からは規制、内部からは自由な場合に
  - ステートフルインスペクション
    必要なポートを一時的に開く
  - パッシブモード
    クライアント側からデータ通信用のポートを開く

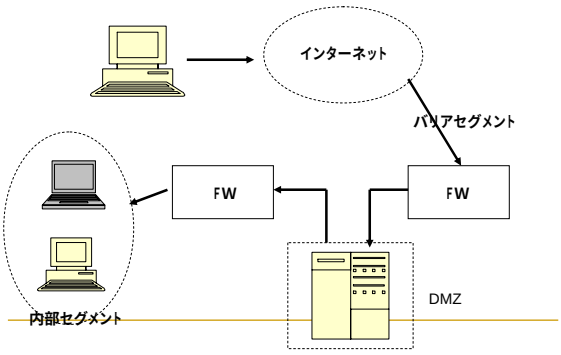
アプリケーションレベルゲートウェイ

- 利用者のアクセスを一旦代理で実行
- 受信したデータの情報とフィルタリングの設定をつきあわせて判断
- パケットフィルタリングよりも高度なアクセス規制が可能
- PROXYサーバと同等
- 外部から個々のIPアドレスが見えなくなる
- 例としてURLフィルタリング（アダルトサイト等）

DMZ

- DeMilitarized Zone、非武装地帯
- 構成要素
  - バリアセグメント
  - 内部セグメント
- 設定方法
  - 2台のファイアウオールで挟む
  - 1台のファイアウオールに2枚のNICを挿してセグメントを分離する

DMZの構成例



暗号化通信

- インターネットでは盗聴される可能性が大
- 暗号化とは特定のルールにしたがってすぐには解読できない文字列に変換すること
- 復号とは元の分に戻すこと
- いずれも鍵が必要になる
  - 共通鍵
  - 暗号鍵／復号鍵
- 解読とは鍵なしで平文に戻すこと（時間がかかることで解読を妨げる）

共通鍵暗号方式

- 暗号化する側、復号化する側が共通の鍵を使用
- 暗号化と復号化は容易
- 人数分鍵が必要
- 鍵をどうやって届けるかが問題
- 鍵を盗まれると、盗聴、なりすまし、改竄などなんでもOK
- 暗号アルゴリズムにDES、3DES、RC4など

DES

- 元の平文を64ビットに区切り、その塊ごとに暗号化
- 鍵長は56ビット
- 3DESは異なる鍵で3回DESを適用

公開鍵暗号方式(1)

- 公開鍵と秘密鍵を使用 (RSA)
- 秘密鍵は手元に自分だけアクセスできるように、公開鍵は相手が取得できるように保存
- 公開鍵と秘密鍵がペアになっている
- 自分(A)の秘密鍵と相手(B)の公開鍵で暗号化
- 相手は自分(B)の秘密鍵と送信者(A)の公開鍵で復号
- 情報漏洩、なりすまし、改ざんを防止可能

公開鍵暗号方式(2)

- 特徴
  - 鍵を秘密裏に交換する必要がないので運用が楽
  - 鍵の数が共通鍵暗号方式に比べて少なくて済む
    n×(n-1)/2 対 2×n
  - 処理が複雑で手間がかかる

電子署名

- 筆跡や音声と違って電子データは送受信者の特徴がない
- 何もしないと、第3者による、なりすまし、改ざんの可能性がある
- 重要な通信をするときは、通信相手と内容が本当に正しいかどうかを判断する仕組みが必要

↓

電子署名

電子署名の仕組み

- 送信者
  - メッセージを作成
  - ハッシュ関数でメッセージを圧縮
  - 圧縮したハッシュ値を送信者の秘密鍵で暗号化する(電子署名)
  - 平文に電子署名をつけて送信
- 受信者
  - データを受信する
  - ハッシュ関数でメッセージを圧縮する
  - デジタル署名を送信者の公開鍵で復号する
  - ハッシュ値を比較する(同じなら信頼できる)

ハッシュ関数

- 原文から固定長の「ハッシュ値」と呼ばれる疑似乱数を生成する
- ハッシュ関数から原文を復元できない
- 128ビット〜160ビット程度の情報として生成
- MD5が有名 (128ビットのハッシュ値に圧縮)
- SHA-1 (160ビットのハッシュ値に圧縮)

MD5(Message-Digest 5)

- RSA暗号化の開発者の一人である Rivest博士らが考案
- 任意の長さのバイト列を 128bit(=16byte)に圧縮
- 基本的には同一の内容からでないと同じ値ができない(詳細は RFC1321)
- 故に MD5で計算した値は元のバイト列の「指紋」のようなものとなり、あるファイルの改ざんの確認に利用可できる
- パスワードの暗号化等でも使用

S/MIME

- Secure/Multipurpose Internet Mail Extension
- 公開鍵方式で暗号化されたメッセージをMIME形式で暗号化して通信

S/MIMEの通信手順

- メール本文をハッシュ化後。送信者Aの秘密鍵で電子署名を生成
- 電子署名とメール本文を合わせて受信者Bの公開鍵で暗号化
- 電子署名と本文を受信者Bの秘密鍵で復号
- 電子署名を送信者Aの公開鍵で復号、復号されたメール本文と比較（なりすまし、改ざん、否認）

SSL

- Netscape Navigator, Internet Explorer
- 個人情報の送受信
  - 会員向け情報提供サービス
  - インターネットショッピング
  - オンラインバンキング
- 公開鍵方式と共通鍵方式を併用
  - サーバ側の証明書だけでサーバ認証

SSLの通信の手順

- httpsでアクセス
- サーバが証明書を送信
- 正当性を確認
- 共通鍵を生成
- サーバの公開鍵で共通鍵を暗号化
- 共通鍵を送信
- サーバが秘密鍵で復号
- Webページを共通鍵で暗号化
- Webページを送信
- 共通鍵で復号化

第三者による証明

- 悪質なインターネット利用者の増加
- ID/パスワードだけではなりすまし防止は難しい
- 信頼できる第三者機構が「間違いなく本人であることの証明」を発行
  - 公的機関　（日本認証サービス、日本ベリサイン）
  - 企業内認証局　（有名企業など）

第三者機関の必要性

- 公開鍵が本当に本人のものかどうか不明
- 通信相手が間違いなく本人であることを証明する機関が必要
  - 日本認証サービス
  - 日本ベリサイン
- それぞれ事前に公開鍵を登録する
- 必要な証明書を事前に発行してもらう

関連キーワード

- 証明書：本人やサービス事業者の証明、電子的な身分証明書
- 認証局：サービス事業者や利用者が本人であることを証明する機関
- 公開鍵暗号：多数／不特定多数の利用者を相手にした時の相手の特定や管理が容易な暗号方式
- 電子署名：原本がどうかを証明するための電子的な署名

デジタル署名の中身

- デジタル証明書によって認証される人は誰か
- デジタル証明書を発行した認証局はどこか
- 公開鍵の種類は何か
- 認証局のデジタル署名

デジタル証明書

- 証明書の種類
  - エンドエンティティ証明書
  - CA証明書
- X.509フォーマット
  - バージョンシリアル番号
  - 署名アルゴリズム
  - 署名者（認証局）
  - 有効期限
  - 公開鍵
  - 認証局のデジタル署名

PKI

- PKIとは公開鍵インフラストラクチャ
- 通信の信頼性を高めるためのインフラ
- 公開鍵が本当に本人のものかどうか
- 認証局（CA）が発行した「デジタル証明書」を使用

政府認証基盤(GPKI)

- 民間の電子商取引の急増
  →行政手続もインターネット経由で行う
- 電子政府構築のミレニアムプロジェクトとして
  1999年11月から2003年度を目標に推進中
- G2B、inG、G2G、G2C

PKIの導入(1)

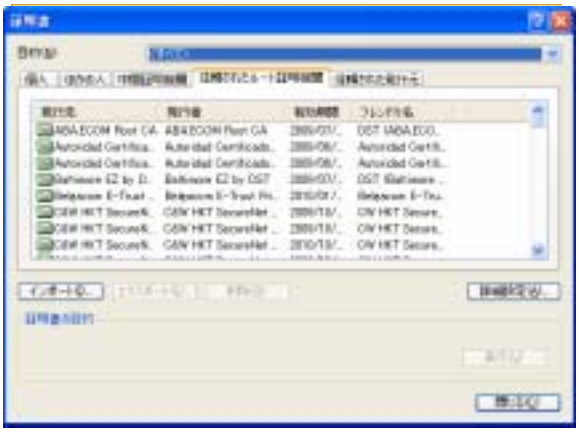
- 対策範囲やレベルを決定
  - 提供するサービスは何？
  - どのくらいのビジネス規模で実施？
  - 守るべき情報は？
  - 不正アクセス時のリスクは？

PKIの導入(2)

- 対策する範囲やレベルに応じた導入
  - 認証局の選定 (委託、企業内)
  - 導入するサーバの選定
  - 認証方式 (サーバの認証、クライアントの認証)
  - 本人確認の方法 (指紋、スマートカード等)
  - 利用者数の調査
  - 暗号化の方式
  - 利用するソフトウェアの選定
  - ユーザアプリケーションへの組み込み方
  - 構築の費用／期間

認証局

- 認証局サーバ
  - 認証やデータの暗号化、電子署名に必要な証明書の発行、管理
- ディレクトリサーバ
  - ネットワーク内の利用者や資源を一元管理
- 登録局サーバ
  - 公開鍵、証明書の一括作成／配布



無線LANのセキュリティ

- ESSID
  - グループ分け
- MACアドレス
  - 接続許可
- WEP
  - ファイル共有
  - Telnet
  - ftp
- SSLとSSH
  - 末端同士の通信を暗号化

債権回収詐欺

- もっともらしい名前で突然請求書を送付
- 心理的な圧迫感を与える
  - もしかしたらと思わせる
  - 赤字で印刷
  - 自宅に直接回収を行う
  - 会社にも訪問する
  - 財産の差し押さえをする
  - 対応する時間がないように配達
- 担当者の連絡先が携帯電話