セキュリティ・ゼミナール
不正アクセス対策とセキュリティツール

1998/12/16

Internet Week 98

白橋明弘

Table of Contents

不正アクセスの手口

不正アクセスの典型的パターン

- Portscan で(不用意に開いてる)サービスを見つけ
- アプリケーションのセキュリティホールを利用し
  (sendmail, INN, phf, imap, pop, rpc.statd, named...)
- /etc/passwd などのファイルを入手し
- パスワードクラックでアカウントを破って
- OSのセキュリティホールをついてroot権限を取り
- トロイの木馬をしこんだり
- パケット盗聴プログラムをしかけたりする

アプリケーションのセキュリティホール

- 最近悪用されることの多いバグ
  - sendmail
  - rpc.statd, named, imapd, qpopper
  - INN
  - CGI のバグ (phf, nph, webdist, count, php, ...)
- ファイアウォールでは防げないバグもあるので要注意

JPCERT/CC活動概要から

- Sendmail への攻撃
- INN を悪用した攻撃
- Web サーバの CGI プログラムを悪用した攻撃
- IMAP サーバを悪用した攻撃
- パスワードの推測、パスワード破り
- ルート権限詐取
- パケット盗聴プログラムによる攻撃
- トロイの木馬プログラム

Sendmailへの攻撃

- 年末年始 sendmail attack
- 国内の多数のサイトに対して sendmail R5 の古典的 security hole をつく攻撃が試みられる
- /etc/passwd をメールで送信し不正に入手
- Anonymous ftp でアップロードを許可する誤設定なども利用
- JPCERT/CC「96年末から97年始にかけての不正アクセスに関する緊急報告」(97/1/9)

INNを悪用した攻撃

- NetNews Server INN の control message を処理するスクリプト parsecontrol のチェック不足をついて、不正なシェルスクリプトを実行させるコントロールメッセージを投稿
- /etc/passwdや/etc/inetd.conf をメールで送信
- それが不正アクセスに結びついた被害は未確認
- この攻撃にはファイアウォールは直接には無力
- JPCERT/CC「ネットワークニュースのサービスを悪用したアタックに関する緊急報告」(97/3/18)

WebサーバCGIを悪用した攻撃

- Web server のバグ付きCGI の “phf” を利用して /etc/passwd を不正入手
- パスワードクラック (辞書引き攻撃) で侵入
- いまだに phf がある Web サイトがある！
- その他 nph, webdist, count, php など多くのCGIバグ

- JPCERT/CC「phf CGIプログラムを悪用したアタックに関する緊急報告」(97/8/5)

IMAPサーバを悪用した攻撃

- University of Washington の imap/pop server の実装に buffer overrun のバグ
- 外部から root 権限でのコマンド実行が可能
- BSD/OS や Linux のパッケージにバグ付きの server が標準装備

- JPCERT/CC「IMAPサーバープログラムを悪用したアタックに関する緊急報告」(97/9/9)

パスワード推測、パスワード破り

- 安易につけられたパスワードを推測
- 不正に入手した /etc/passwd をパスワードクラック (辞書引き総あたり攻撃) にかけ、アカウントを破る

ルート権限詐取

- 一般ユーザのアカウントで侵入を果たした後、オペレーティングシステムのセキュリティホールをついて root 権限を奪取
- 例えば setuid されたプログラムの buffer overrun を利用する

パケット盗聴プログラムの攻撃

- root 権限を得たホスト上で、LAN 上のパケットを盗聴するプログラム (sniffer) をしかける
- 例えば、他のホストへログインするパケットをキャプチャして、ユーザ名/パスワードを盗む
- それを次の侵入の足がかりとする

トロイの木馬プログラム

- システムやアプリケーションのプログラムを、外見はそれまで通りながら不正な機能を果たすプログラムに入れ替える
- アカウントログ関連のプログラムを入れ替えて不正侵入の痕跡の消去やアカウント情報の詐取に利用

サービス妨害攻撃

サービス妨害攻撃

- サーバやサービスを利用不能においこむサービス妨害攻撃 (Denial of Service attack)が深刻化
- TCP/IPやアプリケーションの実装上の問題をつくものが多い
- TCP SYN flood, Ping of Death, OOB, Land attack
- パッチで対応
- TCP/IPレベルのDoS攻撃にはファイアウォールでのアプリケーション(トランスポート)レベルの中継は、一般に有効な防御になる

TCP SYN Flood 攻撃

- TCP の SYN の中途半端な connection を沢山つくられて queue を溢れさせる
- 外部からの接続ができなくなる
- 根本的な対策はない
- TCP SYN Flood による denail of service 攻撃を受けた Web サイト

- CERT Advisory CA-96.21 TCP SYN Flooding

Ping of Death

- TCP/IP の実装のバグをつく
- > 64K の oversize packet を送り付ける
- fragmented packet の assemble で buffer overflow
  > crash/freeze/reboot
- 広範囲なプラットフォームで問題がある
  パッチの存在しないものもある
- Ping だけでなく全てのプロトコルで可能
- Ping o' Death
  http://www.sophist.demon.co.uk/ping/index.html

OOB attack

- Windows NT の port 139 に TCP の urgent flag (Out of Band option) をたてたパケットを送り付けると即死というバグ
- 効果的な Denial of Service 攻撃となる
- NT 4.0 SP3 で対策されたが完全ではないらしい
- 最近は、NT の security hole が多数報告
  - NT がそれだけ使われるようになったため
  - Microsoft も対応にやっきだが...
  - port 137～139 は必ず filtering しておくべき

Chargen/Echo 攻撃

- IPの基本組込みサービス Chargen と Echo を利用した Denial of service 攻撃
- ChargenとEchoをループさせてトラッフックを飽和
- UDP のサービスだとソースアドレス偽造が簡単
- 一昨年 MCI のバックボーンがこの攻撃で麻痺
- CERT Summary で警告

- 不要なサービスは止める/フィルタリングする

LAND attack

- source IP address = destination IP address,
  source port = destination port
  のTCP SYNCパケットを送りつけるとTCP/IPの実装によりカーネルでループしてハングアップ
- Cisco router IOS などが影響をうける
- 設定 (access-list) による回避策がある場合あり
- IP spoofing を伴うので、一般にファイアウォールは有効な防御になる
- CERT CA-97:28 IP Denial-of-Service Attacks

Smurfing

- Broadcast address に対して ICMP echo request のパケットを送る
- Source address は第3者サイトのアドレスに偽造
- 多数の ICMP echo reply のパケットが返される
- ホストおよび回線が麻痺する
- Broadcast に対する ping には応えないようにする
- CERT Advisory CA-98:01 "smurf" IP Denial-of-Service Attacks

ホストの守り方

UNIX がターゲットになる理由

- ネットワークに強い UNIX が狙われる
- きちんと管理すれば、
  決して UNIX のセキュリティは弱くない
- 情報がオープンな UNIX
  - 問題の発見・対策が早い: 両刃の剣
- 標準システムの機能不足は
  フリーソフトの使用などで補える
- WS普及に伴う新米 root の急増が問題

Windows NT/95/98 のセキュリティ

- LAN 環境での使い易さを優先してきたため、セキュリティ上重要な情報を不用意に漏らすことが多い
- デフォールトの設定がセキュリティ的に甘い
- 古いシステムとの互換性のためセキュリティ強化ができない場合がある
- ログに残る情報が不十分なことが多い
- DoS 攻撃の弱点が数多く見つかっている
- Windows 向けクラックツールも盛んに開発される
- リモートログインできないからと安心しないこと

ホストの守り方

- Security hole をふさぐ
  - CERT advisory などをこまめにチェック
  - パッチをあてたり、daemon を入れ替える
- パスワードをしっかり管理する
  - ユーザ教育と Crack 等によるチェック
- 不正アクセスを監視・記録・排除する
  - TCP Wrapper の組込みなどが有用
- 侵入の発見

Security Hole を塞ぐ

- ベンダーから提供されるパッチをあてる
- 危ない daemon などを入れ替える
- buffer overflow vulnerability が危ない
- システム設定を正しく行う
  - 監査ツールの活用
- Security 情報の活用
  - CERT Advisory など
- 「日本語版」での対応の遅れの問題

セキュリティ監査ツール

- 内部監査
  - システムの設定ファイルのチェックなど
  - COPS (Computed Oracle and Password System)
- 外部監査
  - ネットワーク経由で攻撃して弱点をチェック
  - SATAN (Security Administrator Tool for Analyzing Networks)
  - ISS (Internet Security Scanner) など商用の監査ツール
    - Vulnerability DB が命、結果の判断は易しくない

COPSのチェック項目

- Computed Oracle and Password System
- システム関連 file,directory,device のアクセス権
- root およびユーザの設定ファイルのアクセス権
- group,passwd,cron ファイルの内容
- setuid プログラム, など

パスワードの問題 (1)

- 英数記号 8文字
- 暗号化したパスワードを /etc/passwd に格納
- 安易なパスワードは辞書引き攻撃でやぶられる
- 悪いパスワード
  - 辞書(含む日本語)にある言葉
  - 人名,アイドルや近親者の名前・愛称,地名
  - 英文字だけのパスワード
- ユーザ教育の重要性

パスワードの問題 (2)

- パスワード設定時の検査
  - AntiCrack
- パスワードの aging による定期的変更
  - passwd+, npasswd
- Crack などによるパスワード検査
  - 日本むけの辞書とルールの拡張が必要
  - 典型的に数10%のパスワードは破れてしまう

パスワードの盗聴

- パスワードが平文でネットワーク上に流れる
  - 盗聴される危険性がある
- 外部からの login は特に危険
  - Sniffer が仕掛けられている可能性

- One Time Password (使い捨てパスワード)の利用
- SSH, SSL-telnet, PET などの利用
  - 認証と暗号化で安全なリモートログインを実現

アクセス制御 (1)

- 必要のないサービスは止める
- 必要な所にだけアクセスを認める
  - 許可・不許可を判断する条件
    - IPアドレス、ドメイン名
    - ユーザ情報 (ident, dialup/VPN, application での認証)
  - 許可・不許可を判断する場所
    - ルータ、ファイアウォール
    - inetd から呼び出されるサービス
    - アプリケーション

アクセス制御 (2)

- xinetd
  - inetd を置き換え、アクセス制限とログ強化
- tcp_wrapper
  - inetd から tcpd を介してサービスを呼び出す
  - アクセス制限とログ強化 (+コマンド実行)
- ucpspi-tcp
  - inetd 経由でなく、サービス毎に tcpserver がデーモンとして常駐してサービスを呼び出す

ロギング機能

- コネクションのログ
  - tcp_wrapper などの提供するログ機能
- アプリケーションのログ
  - 認証の成功･失敗、コマンド実行の内容･結果
  - ログが十分に残らないデーモンは交換する
- logdaemon
  - telnetd や rlogind のログ機能を強化
  - 使い捨てパスワード(S/Key, OTP)のサポート

侵入の発見 (1)

- Tripwire によるシステムの integrity check
  - 改変されているファイルを見つける
  - ファイルの属性と message digest を定期的に検査してデータベースと比較し、変更点をレポート
  - ディレクトリ毎のチェック内容を細かく指定できる
  - Tripwire のシステムとデータベースは readonly ないしは offline の安全な場所に保存すること

侵入の発見 (2)

- network interface の status
  - promiscuous mode にある → sniffer の疑い
  - cpm (check promiscous mode) でチェック
- 各種ログのチェック
  - watcher や swatch でログ監視を自動化
  - ログ出力中の特定のパターンを監視し、メールで通知や指定コマンド実行などを行う汎用ツール

Intrusion Detection System

- ネットワーク上の通信を監視しアタックを検出
  - 管理者に通知、さらに遮断 (Shunning) も行う
- 課題もある
  - Detection System の裏をかく手法の開発
    low bandwidth scan, distributed scan
  - DoS アタックを仕組まれる危険性
- フィイアウォールとは補完的であり、ファイアウォールの使えない状況では有効

ファイアウォールの活用と限界

ファイアウォールの考え方

- Internet の基本は end to end の接続性
- しかし，多数のホストは守りきれない

- 壁 - Firewall - を設けてそこで食い止める
- 外部からのアクセスは必要最小限のものに限定
- 壁の外におくのは少数のホスト → 厳重に守る
- サービスは壁を越えて利用できるようにする

ファイアウォールの限界

- ファイアウォールで防げない攻撃もある
  - 電子メール爆撃
  - メール、Web によるウィルスの感染
  - 危険な downloadable object (Java, ActiveX)
  - Webブラウザのバグ
- ファイアウォールの限界を知ることが重要
  - アプリケーションのバグへの対応
  - サービス妨害攻撃への対応
  - コンテンツフィルタリングへの対応

アプリケーションのバグの対応

- ファイアウォール上で安全な中継を行う
- 全てのアプリケショーンのプロトコルの内容の正当性を保証することは不可能
- 例えばINNのケースのように、アプリケーションのセキュリティホールには対応できないケースも多くある
- ファイアウォールの飛び越し
- その後の攻撃者の活動はファイアウォールによって大幅に制限されるので、無意味ではない

コンテンツフィルタリングの対応

- ファイアウォール(ゲートウェイ)のフィルタリング
- SPAM
  - ブラックリストの管理が課題
- ウィルス
  - 実用的なレベルに達している
- Java/ActiveX
  - これからの課題
- URL filtering
  - セキュリティの話題ではないが、需要はある

安全なアクセスのための技術

認証の方法

- 認証技術の分類
  - ある知識を知っていることによる認証
    パスワード、暗証コード
  - ある物を持っていることによる認証
    IDカード、鍵、電話番号
  - ある特徴を持っていることによる認証
    諮問などの生体計測 (Biometric)

固定パスワードと使い捨てパスワード

- 2種類のパスワード方式
  - Reusable Password (固定パスワード)
    パスワードを知られると Replay 攻撃の危険性
  - One Time Password (使い捨てパスワード)
    知られても再利用できないので安全
- よくある誤解
  - Reusable Password ≡ 平文パスワード ではない
  - OneTime Password ≡ 暗号パスワード ではない

OneTime Password

- Challenge Response 型
  - ホストからの challenge
  - "Local で" password を入力し演算
  - 結果を response として送る
- 同期型
  - 時刻またはカウンターで同期をとる
  - challenge の替りにシードとして時刻/カウンタを使う
- One Time Password の例
  - S/Key, OTP, TokenCard

S/Key の例

- s/key 4979 ux0-sv

  ここを OTP Paramters (challenge) として入力
  Secret Password とあわせて
  One Time Passphraze を計算して

- Password: *VAIN ROT MESS DARE JUKE HOSE*

  結果を Password (response) として入力
  入力がし易いように、英単語風に変換

Token Card

- SecurID (by Security Dynamics)
  - 時刻同期方式、豊富な実績と対応アプリケーション
- SafeWord (by Secure Computing)
  - Challenge/Response とカウンター同期の2モード
  - ANSI X9.9 で他のカードと互換性
  - ミラーサーバによる冗長構成
- SecureNetKey (by AssureNet)
  - Challenge/Response のみ
  - 使い易い管理およびログ分析ツール

One Time Password を使い易くする

- ワンタイムパスワードは面倒→使われない
  - Challenge/Response は特に敬遠されがち
- S/Key, OTP の自動入力ツール
  - dotkey95, optsock for Windows 95
    http://tama.gate.nec.co.jp/so/
  - Challenge を Cut&Paste または自動監視でパスフレーズの入力ボックスがポップアップする

Internet からリモートログイン

- 安全な認証と暗号化が必要
- 平文パスワードは Monitoring Attack の餌食に

- リモートログイン
  - One Time Password による telnet, ftp の利用
  - SSL-Telnet
    SSH (Secure Shell)
  - PET (Privacy Enhanced Telnet)
  - VPN (IPSec, PPTP) によるリモートアクセス

SSH (Secure Shell)

- SSH = Secure な r-コマンド
  - 暗号化 DES/Triple-DES/IDEA/RC4
  - 認証　RSAを用いたチャレンジ＆レスポンス
    - サーバが256bitの乱数を公開鍵で暗号化して送る
    - クライアントが秘密鍵で復号化してMD5値を送り返す
- port forwarding の仕組み
  - SSH上で X-window や POP なども使用可能
  - VPN のように全てのアプリケーションが透過的に使えるわけではない

Windows用 SSH クライアント

- SSH の普及には Windows クライアントが鍵となる
- win32 コマンドライン版
- Cedomir Igaly 氏の SSH Windows Client
  - なかなかよく出来た GUI のクライアント
- 商用の F-Secure
  - アプリケーションの起動などの工夫で使い易い
- TeraTerm SSH plug-in
  - リモートログイン用としては日本語対応のこれがお薦め

SSL-telnet

- SSL-telnet = SSL化された telnet
  - 暗号化のみ、認証は未対応
- Windows用クライアント
  - STelSock + SSLeay + TeraTerm
  - stone + SSLeay + TeraTerm
  - SSL-TeraTerm with SSLeay
- SSLeay Eric.A.Young氏によるフリーなSSLの実装
  - FAQ日本語訳 http://www.infoscience.co.jp/technical/crypto/ssleay_jp.html

Internet からメールアクセス

- 内部メールサーバへのアクセス
  - POP では平文パスワードが盗聴される恐れ
- APOP
  - Challenge & Response によるパスワード暗号化
  - サーバ: qpopper, DeleGate
  - クライアント: EudoraPro, Winbiff, Becky!, AL-Mail32
- WWW/Mail gateway の利用
  - WebMail, CGIMailer, メールサーバのWebサービス
- SSL-POP, SSL-IMAP, VPN による暗号化

Webのセキュリティ

Downloadable Object の Security

- WWW の高機能化に伴う危険の増大
  - External Viewer (sh, postscript, Word, PowerPoint)
  - Plug-in (Shockwaveでe-mailが読めるホール)
  - Java、JavaScript, ActiveX (ホール多数)
  - Cybernotのセキュリティホール(*.url, *.lnkで実行)

- WWW Security FAQ: Client Side Security
  http://www.w3.org/Security/Faq/www-security-faq.html
  http://www.jkaabl2.kais.kyoto-u.ac.jp/www-secu.html

Java,JaveScript のセキュリティ (1)

- JAVAセキュリティ/プリンストン大SIPチームの研究
  - 実装上の欠陥
    - 仮想マシンのバグ、クラスライブラリのバグ
  - 設計上の欠陥
    - セキュリティモデルの定義が無い
    - バイトコードの形式的な検証が可能でない
  - DNS詐称により、アプレットをダウンロードした以外のホストと通信ができる
- JAVAセキュリティ/G.マグロー,E.フェルテン/トッパン

Java,JavaScript のセキュリティ (2)

- プライバシ問題
  - ユーザの名前で電子メールを勝手に送信する
  - ユーザのURLアクセス履歴にアクセスする
  - ユーザがアクセスするURLを監視する
- 仕事妨害攻撃
  - CPUやメモリを大量消費、ウィンドウを無数に開く
- 詐欺行為
  - ユーザ名･パスワードを盗む偽ウィンドウを作る
  - ブラウザの表示するURLの情報をごまかす

Web ブラウザのセキュリティホール

- プライバシ情報の流出
  Preferences問題(NS), FreiBerg問題(IE)
- アクセス情報の追跡･監視
  Tracker問題(NS), Bell研指摘の問題(NS,IE)
- 許可されない通信
  Javaリダイレクト問題(NS,IE)
- 悪意あるコード･プログラムの実行
  URLバッファオーバーラン(IE), Cybernot問題(IE)
- 予期せぬローカル資源へのアクセス
  Danishプライバシ問題(NS), Javaキャッシュ問題(IE)

CGI セキュリティ

- CGIプログラミング上の注意
  - 不用意にシェルを呼び出さない (system より exec)
  - ユーザが入力する全ての値をチェックする
    - 有効な文字種だけを通す(メタキャラクタをフィルタ)
    - 引数の長さ、引数の値の妥当性をチェックする
  - システム関数に渡す引数、戻り値をチェックする
  - 誰でも書き込みできるディレクトリにファイルを作成しない
  - カレントディレクトリや相対パスは信用しない
  - プログラムをコアダンプさせない
  - できるだけ多くの情報をログに残す

SPAMメール対策

SPAM メール問題

- 深刻なSPAMの被害
- SPAM対策 (1)
  - 自ドメインが受け取るSPAMメール対策
- SPAM対策 (2)
  - SPAMメールの中継に利用されない対策

深刻な SPAM の被害

- SPAM メール
  - 多数のユーザを標的にばらまかれる商業メール
  - 出す側のコストは非常に安い
  - アドレスを集めて売ったり、SPAM配送を引き受ける業者の登場
    - 3,500万アドレスがたったの$35
  - 受け取るユーザやISPがコストを負担させられる
  - 米国では、訴訟やInternetからの「締め出し」も

SPAM 対策 (1)

- 自ドメインが受け取るSPAMメール対策
  - SPAMアドレス、SPAMドメインからの受信を拒否
    - ブラックリストの管理
    - VIX/MAPS RBL や DORKSLAYERS/ORBS の利用
  - 送信元アドレスが実在することの確認
    - 送信元アドレスを DNS でひいて、メール reachable でない場合は受信を拒否
    - 悪意はなくても正しい送信元アドレスが設定されていないメールは受け取れなくなってしまう

SPAM 対策 (2)

- SPAMメールの中継に利用されない対策
  - 外から入ってきて外へ出ていくメールは拒否する
    - ISP等では必須の設定となっている
    - 放置していると抗議が殺到するだけでなく、SPAM中継サイトとしてブラックリストに載せられてしまう
    - 別のISPからメールサーバを使いたいユーザは不便
    - POP接続後だけSMTPを受け付ける対策
  - 中継時にヘッダにトレース情報をきちんと残す
    - 配送元ホスト名、IPアドレス、配送先メールアドレス

Mailing List 運用の注意

- SPAMやe-mail爆撃に利用されないよう要注意
  - SPAMメールをML宛に投げ込まれる
    →登録者(メンバ)以外からの投稿は受付けない
  - メンバーリストが別の目的に利用される
    →メンバのe-mailアドレスのリストは公開しない
  - メーリングに本人の承諾なしに登録されてしまう
    →自動登録は管理人経由かconfirm付にする

付録

参考記事、参考URL

参考記事

http://www.netone.co.jp/doc/index.html

- インターネット･セキュリティ概論
- ファイアウォール導入の手引き
- PC環境におけるセキュリティ -電子メールを中心に-
- セキュリティのためのプロトコル
- インターネットセキュリティその現状と対応
- セキュリティポリシーの決定とファイアウォールの選び方

http://www.jpcert.or.jp/magazine/beginners.html

- 初心者のためのセキュリティ講座 by JPCERT/CC

参考 Internet Week 97 Tutorials

- 97/12/16 インターネットセキュリティ(1) 岡田高
  http://www.nic.ad.jp/iw97/tutorial1/okada-sec1.pdf

- 97/12/17 インターネットセキュリティ(2) 歌代和正
  http://www.nic.ad.jp/iw97/tutorial2/security2.pdf
- WIDE School of Internet Project によるVODでの提供
  http://www.sfc.wide.ad.jp
  /soi/iw97/iw97_tut/slides/07/01.html

参考URL Web Security & SSH

- SSL-Talk FAQ
  http://www.consensus.com/security/ssl-talk-faq.html
- SSL Q&A
  http://robin.sl.cae.ntt.jp/~motoda/SSL/FAQ/
- W3C Security Resource
  http://www.w3.org/pub/WWW/Security/
- WWW Security FAQ
  http://www.w3.org/Security/Faq/www-security-faq.html
  http://www.jkaabl2.kais.kyoto-u.ac.jp/www-secu.html
- SSH FAQ
  http://www.vacia.is.tohoku.ac.jp/~s-yamane/FAQ/ssh

参考URL Windows Security Tool

- ftp://ftp.aist-nara.ac.jp
  /pub/Security/tool/otp-commands/win/
- http://tama.gate.nec.co.jp/so/
- http://www.infoscience.co.jp/eng/products/sslterm/
- http://www.gcd.forus.or.jp/sengoku/stone/
- http://guardian.htu.tuwien.ac.at/therapy/ssh/
- http://public.srce.hr/~cigaly/ssh/
- http://www.geocities.com
  /SiliconValley/Bay/1692/ssh-index.html
- http://www.zip.com.au/~roca/ttssh.html

参考URL SPAM

- 電子メール配送プログラムの不正利用
  http://www.jpcert.or.jp/tech/97-0001/
- SPAM Information Page
  http://caramia.g-net.org/spam/
- ANTI UCE (Unsolicited Commercial Email)
  http://www.ayamura.org/mail/
- Limiting Unsolicited Commercial Email
  http://www.imc.org/imc-spam/
- Fight Spam on the Internet!
  http://spam.abuse.net/