帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

コンピュータ概論(5)
セキュリティ

中野秀男
帝塚山学院大学非常勤講師
大阪市立大学名誉教授、堺市情報セキュリティアドバイザ

今日の話

- リアルタイム・ネット講義について
- 教科書11章「セキュリティ」図を使いながら
  - 11.1 悪意のあるソフトウェア
  - 11.2 攻撃方法
  - 11.3 暗号
  - 11.4 認証
- 追加の話と息抜きに
  - 情報セキュリティ論からピックアップして
  - 作家の高村薫さんの「神の火」
- コメント用紙の代わりにC-Learningのレポートに
  - 一旦、ネット講義を止めてレポートに書く時間も
  - 質問によっては、このネット講義で説明します

11.1 悪意のあるソフトウェア(1)

- 11.1.1 マルウェア
  - コンピュータシステムに対して不正な動作を行うソフトウェア
  - 図11.1 マルウェアの分類(p.173)
- 11.1.2 コンピュータウィルス
  - 宿主プログラムが必要で増殖機のをもつ(図11.2, p.174)
  - ワーム：増殖機能をもつ
  - トロイの木馬：増殖機能を持たない
    - スパイウェア、バックドア

11.1 悪意のあるソフトウェア(2)

- 11.13 ワーム
  - メールに添付して増殖(アドレス帳などを使って)(図11.3, p.174)
  - ボット：遠隔からの指令動く。スパムメール、DDoS攻撃
    - 図11.4, p.175)
- 11.1.4 トロイの木馬
  - スパイウェア：コンピュータの中にある個人情報などを盗む
  - バックドア：悪意のある攻撃者が不正に制御
  - ログインのトロイの木馬(古典的)
- 11.1.5 バックドア
  - 中国製製品への不安

11.2 攻撃方法(1)

- 11.2.1 不正侵入
  - コンピュータに対してアクセス権のないユーザが不正に操作
  - セキュリティホールをついてくる
    - こまめにバージョンアップしましょう
  - バックドアがあると入られる
- 11.2.2 踏み台攻撃(図11.5, p.176)
- 11.2.3 DoS攻撃
  - サービス不能攻撃 : Denial of Service
  - ウェブへの同時大量アクセス : コンピュータやネットワーク帯域
    - 送信IPアドレスを止めるが、、
  - DDoS: 分散DoS攻撃(Distributed DoS) 図11.6, p.177

11.2 攻撃方法(2)

- 11.2.4 セキュリティホール
  - アプリやOSでプログラムの不具合や設計上のミスで発生した欠陥
  - ウェブの改ざん：バッファーオーバーフロー攻撃
- 11.2.5 対策
  - アカウント管理をしっかり：アクセスログも監視
  - パスワードを強固にする
  - OSやアプリのアップデートはしっかり
  - 不審なメールの添付ファイルは開かない
  - 信用できないウェブサイトは閲覧しない
  - ウィルス対策ソフトとデータの更新
  - ファイヤーウォール装置やソフトウェア(図11.7, p.178)

11.3 暗号(1)

- 11.3.1 暗号に関する用語
  - 符号化(encoding):データを規則にしたがって変換
    - 復号(decoding);元のデータに戻す
  - 元の文(データ):平文(ひらぶん)(plain text)
    - 暗号化(encryption):暗号文(cipher text)
  - 復号(decryption):暗号文を平文に戻す
  - 暗号解読:正規のユーザでない人が復号する
  - 鍵:
    - 暗号鍵:暗号化するための情報
    - 復号鍵:復号するための情報
  - 暗号アルゴリズム:暗号化や復号の手順や規則

11.3 暗号(2)

- 11.3.2 暗号技術の発展
  - 2000年前のローマ時代のシーザー暗号：k文字ずらす
    - 換字、転置
  - 1970年代までは暗号鍵も複合鍵も秘密にする慣用暗号だけ
    - 暗号鍵と複合鍵が同じなので共通鍵暗号ともいう
    - 有名なのはDES、今はAES
  - 1970年代後半に片方の鍵を公開する公開鍵暗号
    - 有名なのはRSA暗号
    - これで電子ショッピングとかが安全に
  - 今は最初、公開鍵でセッションの共通鍵(慣用暗号)を交換して、通信は高速な共通鍵(慣用暗号)を使って行う

11.3 暗号(3)

- 11.3.3 共通鍵と公開鍵
  - 共通鍵方式：暗号鍵と複合鍵を一緒にして秘密に
    - データの秘匿化に使う(図11.8, p.179)
    - 古くはDES暗号：鍵が56ビットなので解読される
    - 今はTriple DESやAES(Advanced Encryption System)
  - 公開鍵暗号：暗号鍵と復号
  - 鍵を一対にして片方を公開
    - 秘匿化：暗号鍵を公開(図11.9, p.180)
    - 電子署名：復号鍵を公開
    - RSA暗号： Rivest, Adleman, Shamir
      - 200桁の複合数を100桁程度の素数の掛け算で
      - 200桁の複合数の素因数分解は難しい

11.3 暗号(4)

- 11.3.3 ハッシュ関数
  - 任意の長さのデータから固定長のデータを出力する
    - 辞書なんかがわかりやすい：帝塚山学院大学を「帝」から検索
  - 暗号と違って元に戻らない
    - 個人情報秘匿のための匿名化処理に使える
    - 電子署名にも使える
    - プログラムの改ざん防止にも
  - ハッシュ関数でできたものが「メッセージダイジェスト」
- 11.3.4 ハイブリッド暗号
  - 共通鍵は高速、公開鍵暗号は処理に時間がかかる
  - それを組み合わせてハイブリッド暗号
    - セッション鍵の共通暗号を公開鍵暗号方式で交換
    - やりとり(セッション)は共通鍵を使う

11.4 認証(1)

- 11.4.1 電子署名
  - 改ざん防止、なりすまし防止、否認防止に使う
  - メッセージダイジェストを用いた電子署名(図11.10, p.181)
    - 秘匿性はない
  - ハイブリッド暗号(図11.11, p.182) 秘匿性と電子署名を実現
- 11.4.2 公開鍵基盤 : PKI(Public Key Infrastructure)
  - 図11.12, p.183
  - 利用者(Aさん)は認証局(CA)に証明書を発行してもらう
    - CA: Certification Authority): 有名なのはVeriSignなど
  - 利用者(Xさん)はAさんをリポジトリに問い合わせて、Aさんが有効であることを確認して、Aさんの公開鍵を手に入れる
  - 証明書がおかしければ証明書失効リストをレポジトリーに

11.4 認証(2)

- 11.4.3 個人認証
  - 個人認証の三要素
    - 本人の知識(知っていること):パスワードや暗証番号
    - 本人の持ち物:物理的な鍵、カード
    - 本人固有の特徴:指紋、顔、音声、筆跡(バイオメトリックス)
  - パスワード
    - 長さ、大文字小文字記号
    - 利用者の情報をあまり使わない
    - 定期的な更新(aging)
    - 今は二重、多重認証が普通なので、パスワード不要論も

旬の話：「情報セキュリティ論」から

- 今年の「情報セキュリティ論」
  - 情報セキュリティの定義
  - セキュリティ対策は
  - 公開鍵暗号とそのインパクト
  - 認証の要素
  - パスワードその後
  - 情報セキュリティの変遷
  - 最近の情報セキュリティの考え方
  - 標的型攻撃：定義と目的

情報セキュリティの定義(2回目スライド11)

- 情報セキュリティはCIA
  - OECDの定義
- C: 機密性：秘匿
  - 情報を見られたり盗まれた場合の損失
  - Confidentiality
- I: 完全性：中身
  - 改ざんなどによる影響
  - Integrity
- A: 可用性：運用
  - サービス停止やパーフォマンス不足による影響
  - Availability

セキュリティ対策は（続）(2回目スライド16)

- ユーザにとって
  - 幾つかのパスワード
  - 多重認証を使う
    - パスワード以外にIDカードや電話番号認証や端末認証を併用
  - コンピュータウィルス等の防御ソフト
  - 標的型攻撃メールに気をつける
    - 一般的にはおかしい添付ファイルやURLは開かない
  - プライバシー漏洩対策
- 管理者にとって
  - たくさんあります

公開鍵暗号(4回目スライド4)

- 暗号解読の難易度を数学的に示す
- １方向性関数（逆計算が難しい）を利用
- RSA暗号(Rivest,Shamir,Adleman)
  - 合成数の素因数分解の難しさが暗号の強度
- 処理速度は一般的に慣用暗号より遅い
- 秘匿化だけでなく署名(認証)にも使える
- 電子署名だけならハッシュ（Hash)も使える
  - ハッシュは暗号と違って元に戻らない
  - 戻らない利点を使って匿名化技術に

公開鍵暗号のインパクト(4回目スライド5)

- 暗号が秘匿化だけでなく認証に使える
- デジタルなものに電子署名
- インターネット上でビジネス
- 慣用暗号と組み合わせると実用的
  - 鍵の交換は公開鍵
  - データ伝送時は慣用暗号
- 数学的な難しさに依存する安心感

認証の要素(5回目スライド7)

- 身体情報(Something You Are)
  - バイオメトリクス（指紋、虹彩、顔、音声、筆跡）
  - マシンの場合は（IPアドレス、MACアドレス）
- 知っている事(Something You Know)
  - パスワード、パスフレーズ、暗証番号
- 持っているもの(Something You Have)
  - IDカード、RFID(無線タグ)

パスワードその後(2) (6回目スライド7)

- パスワードだけは、もうダメなので多重認証
- 多くはパスワードや暗証番号以外に他の認証も
  - 二重認証、多重認証
- 例
  - 他の端末でも認証
    - 番号を送る(One Time Password)
    - ログインをしたことを知らせて、おかしければアクションを
  - 暗証番号とカードの代わりにカードと生体認証
- いずれは体にマイナンバーを埋め込むのかなあ！

情報セキュリティの変遷(8回目スライド3)

- 歴史的に
  - 1980年ぐらいまでは暗号(慣用暗号)
  - 公開鍵暗号の登場で電子署名などビジネスや暮らしに
  - 1990年代のインターネットの普及でセキュリティが重要に
- 今
  - 国や企業を狙ったインシデントが
  - コンピュータ犯罪からサイバー犯罪へ
  - 国と国などとのサイバー攻撃合戦(第5軍)
  - 標的型攻撃/標的型攻撃メール

最近の情報セキュリティの考え方(8回目スライド4)

- セキュリティ原理主義者に対して
- IT/ICTを最大限に使うためのセキュリティ
  - 投資
  - それ以上は犯罪という切り分け
- プライバシは世界の流れも
  - 米:トラッキング禁止(Do Not Track)
  - 欧:忘れてもらう権利(Right to be forgotten)→消去権
  - IT/ICTも世界のレベルで動いている
- 法律がIT/ICTに追付いてきた
  - 有罪と無罪を切り分ける法律と裁判
- IoT時代のセキュリティ

標的型攻撃(1)定義と目的(8回目スライド6)

- 組織はそこそこ強くなったので、まず弱い個人から攻めよう
- 定義
  - 明確な意志と目的をもった人間が、特定のターゲットに対して、特定の目的で行う、サイバー攻撃の一種
  - 欧米ではAPT(Advanced Persistent Threat)
- 目的
  - 政治的活動(Anonymous, WikiLeaks)
  - サイバー犯罪
  - サイバーテロ
  - サイバー戦争(サイバー空間は第5の戦場)
  - 業務妨害(DDoS攻撃によるサーバ停止)
  - 政治的駆け引き
  - 個人的な動機による攻撃

セキュリティ関係の用語集

- IPAのセキュリティ用語集
  - https://www.ipa.go.jp/security/glossary/glossary.html
  - ネットワークセキュリティ関連用語集
  - PKI用語集
  - コンピュータウィルス用語集
- セキュリティ用語事典@IT
  - https://www.atmarkit.co.jp/ait/subtop/features/kwd/security_glossary.html

高村薫さんの「神の火」

- 直木賞作家「マークスの山」1993年
  - 大阪の人なので知った地名が
- 「神の火」は2作目 1992年
  - このセキュリティ関係で取材を受ける
  - 作品の中では梅田コンピュータ学院の山田講師で登場