帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

コンピュータ概論(14)
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

1

今日の話

- 第11章 セキュリティ
  - 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
- 高村薫さんの「神の火」

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2

11.1 悪意のあるソフトウェア(1)

- インシデント(事件または事故)
  - 脅威と脆弱性があってリスクが発生し
  - 攻撃があるとインシデントが発生する

- 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

3

11.1 悪意のあるソフトウェア(2)

- 11.1.3 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
- 11.1.4 トロイの木馬
  - スパイウェア:
    - コンピュータにある個人情報などを盗む
- 11.1.5 バックドア
  - 他からアクセスできるような仕組み
  - 中国製製品への不安

4

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

5

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
      - gets()
      - Null: ストッパー
  - セキュア・プログラミング

6

11.2 攻撃方法(3)

- 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)

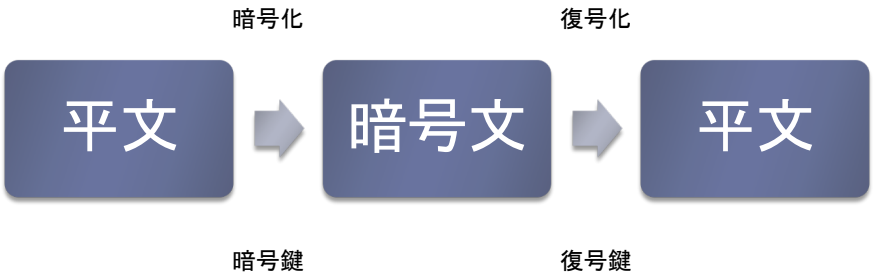
7

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

8

暗号の言葉



9

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復号鍵も秘密にする慣用暗号だけ
    - 暗号鍵と復号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

10

11.3 暗号(3)

- 11.3.3 共通鍵と公開鍵
  - 共通鍵方式：暗号鍵と復号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

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

12

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

13

11.4 認証(2)

- 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

14

11.4 認証(3)

- 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
    - パスフレーズ:PGP(Pretty Good Privacy)

15

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

16