帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

コンピュータ概論(13)
セキュリティ

中野秀男
情報メディア学科

今日の話

- 質問と回答(1) 軽く前回の講義関連
- セキュリティ
  - 情報セキュリティ論のスライドを使って説明
    - 「情報セキュリティ概論」はVOD講義で公開しています
    - 「中野秀男研究室」のウェブの担当講義
  - 基本的な考え方
  - 基礎：暗号、認証
  - 最近のセキュリティ：サイバー犯罪、標的型攻撃
  - SNSのセキュリティやプライバシー
- 旬の話：Android(途中で)

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

質問

- 自動運転のレベル
- 災害は今の技術で防げるか
- ドローンが発達すると災害地に救援物質が
- このままコンピュータが教科書になることはあるか
- ビットコインは持ってないのか
- コンピュータウィルスはどうして見つかるのか

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

セキュリティの定義: CIA

- 欧州のOECDの定義
  - 情報システム及びネットワークのセキュリティのためのガイドライン
- Confidentiality
  - 機密性：秘匿性、アクセス制御、暗号
- Integrity
  - 完全性：中身が変わらない、保証されている
- Availability
  - 可用性：サービス停止やパーフォマンス不足がない

情報セキュリティの変遷

- 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
  - 国と国や国と組織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
    - 組織やあなたを目掛けて

最近の情報セキュリティの考え方

- IT/ICTを最大限に使うためのセキュリティ
  - 投資
  - リスクマネジメント
  - 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→GDPR
    - GDPR(General Data Protection Rule) 2018年5月25日から
  - 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

セキュリティは計れる

- セキュリティに万全はない
- 強いセキュリティ、弱いセキュリティ
- 守る/破るのに必要なリソースの量
  - お金、時間、能力
- 例
  - 番号合わせの鍵
  - 暗証番号（4桁）
  - パスワード
- でもそれぞれに抜け道はある
  - 知恵との戦い
  - 世界に70億弱の人がいる
  - これからはAI(人工知能)も参画

インターネットのセキュリティ

- 理論というより箇条書きの世界
  - 攻められながら改善されている
  - セキュリティ x 利便性 ＝ 技術力 x 運用力
  - 守るツールと破るツールは表裏一体
- 時代の変化とその先
  - SOHO、モバイル時代のセキュリティ技術
  - ユビキタス時代のセキュリティ、プライバシ
  - ソーシャルメディア時代のセキュリティ
  - IoTのセキュリティ
    - IoT: Internet of Things(もののインターネット)

セキュリティ対策は

- 1. 技術
  - まずは、出来るところまで
- 2. 規則、法律
  - 後追いだが、定まれば強力
  - 法律がITに追付いた
- 3. モラル、倫理、教育
  - 長い目で見れば、
- 保険もあります

セキュリティ対策は（続）

- 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

暗号の歴史

- 古くはシーザ暗号：文字を数文字シフト
  「NAKANO」→「OBLBOP」 1文字シフト
  英語の大文字26文字だけ使用
  - 暗証番号程度なら便利
- 換字と転置の組み合わせ
  - 換字：文字を変える
    - 頻度分布解析で簡単に解読：E,TH,HE,THE
  - 転置：文字順の入れ替え
    - もとの字が残る：「なかの」→「のなか」

暗号の歴史（続）

- 1970年後半まで（公開鍵暗号の出現まで）
  - 鍵を秘密にする：秘密鍵暗号→慣用暗号
  - 第1次、第2次世界大戦までの暗号
    - Enigma
  - 戦争の歴史：暗い暗号研究
- 1980年以降（公開鍵暗号出現以来）
  - 暗号の利用範囲が多岐に（署名にも）
    - 電子署名→電子商取引
  - 慣用暗号と公開鍵暗号の長短所を使って併用
    - 鍵の交換を公開鍵で、データ伝送は慣用暗号
  - ビットコインやブロックチェーンも公開鍵暗号を利用

暗号の言葉

暗号の種類

- 慣用（共通鍵）暗号
  - 暗号化鍵も復号化鍵も秘密（秘密鍵）
  - 1980年前までは、暗号はこれだけ
- 公開鍵暗号
  - 暗号化または復号化鍵を公開する暗号
    - もう1つの鍵は秘密
  - 暗号化鍵を公開：秘匿
  - 復号化鍵を公開：電子署名
  - ビットコインでも公開鍵が使われている
    - 公開鍵が受け取りアドレス
    - 秘密鍵が取引(売買)用：かいざん防止

認証とは

- 認証とは
  - 私があなたを中野さんだと認めること
  - ATM端末があなたが正当なバンクカードの持ち主と認めること
  - AがBを正当な相手だと認めること
- AやBは人（ユーザ）、マシン？
- 正当の定義は
  - 人と物では違う
- どうすれば認めたというか？

認証の要素

- 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(1)

- システム管理者やっていると多くのパスワード
  - 普通の人でも最近はいくつかのパスワード
    - 三つぐらいがいいのでは
  - 私の場合は
- これからはパスワードとIDカードか？
  - セキュリティレベルに応じて身体情報も
- 増える One Time Password(OTP)
  - Secure Card：ユーザとホストが乱数を共有
  - S Key: ランダムに生成した乱数を最後から使用
    - 一方向性関数で生成
  - ネットバンキングなど

パスワードその後(2)

- 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！

旬の話:Android

- GoogleがAndroidソフトをオープンソースソフトウェアとして公開
- 多くの企業がAndroidソフトを使ってAndroidデバイスを
  - Androidスマホ
  - Androidタブレット
  - ロボホン
  - MOVERIO
- 基本は同じだが各社、各製品で独自の部分も
- Apple系はハードもAppleのみ
  - ソフトの原則としてApple Storeで

標的型攻撃(1)定義と目的

- 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

標的型攻撃(2)目的(続)

- サイバー犯罪
  - オンラインバンクを利用しての不正送金
    - 最近は二重認証の方向へ
  - フィッシング詐欺(Phishing)
  - ランサムウェア(Ransomware)による脅迫：身代金ウィルス
  - 個人情報の売買
  - DDoS攻撃
- 個人的な動機による攻撃
  - 愉快犯
  - 恨みつらみ
  - サイバーストーカー

標的型攻撃(3)標的型メール

- 実体
  - 業務連絡を装ったメール
  - 取引先を装ったメール
  - 冠婚葬祭を装ったメール
  - 時事ニュースを装ったメール
  - 人材募集を装ったメール
  - グリーティングカードを装ったメール
- 不正プログラムの実行
  - 添付ファイル
  - URLのクリック(不正サイトへの誘導リンク)

個人情報

- 最初の個人情報保護法は基本4情報
  - 名前、性別、生年月日、住所
- 法律が改定されて、
  - 個人情報:個人を特定する情報と、個人の情報
  - プライバシーは「要配慮個人情報」
- 個人識別子
  - 指紋データ、顔認識データ
  - クレジットカードや共通ポイントカードの会員番号
  - 一社単独のポイントカードの会員番号
  - 登録制ウェブの会員番号
- 罰則が6ヶ月以下の懲役か、30万円以下の罰金
- 処理情報と散在情報
- 個人特定性低減データ、匿名加工

私の場合

- 公開と制限付き公開
  - 予定表
    - AppleのiCloud
  - 日記
    - Mixi, ココログ
  - Twitter, Facebook
    - Twitterは私人用と大学宣伝用
    - Facebookは公人: 位置や状態(近況)を
- プライベート
  - お仕事(ToDo)表: Remember The MilkとNumbers(Excel)
  - 健康(血液検査のデータ)Dropbox
  - 小遣い帳(その場で入力と月末の集計)と収支

Mixi

- 日記
  - 私は2004年9月27日「ほろ酔い日記」
  - 今は6つのブログにも
- 友人(私は126名):いくつかのグループに
- コミュニティ(私は33件に参加)
  - 管理人
- 匿名、ハンドル名あり
- 私は日記と、Mixiをメインにしている友達用
- 幾つか事件も
  - 関東方面の大学

Twitter

- 短文(140文字)投稿サイト
- フォローとフォロワー
  - 私は2009年11月1日からハンドル名で
  - 途中から非公開に
  - プライベート利用
  - 今は大学用も作って宣伝、同時にFacebookとインスタも
- TL(Time Line):これがポイント
- デフォルトは公開
  - **Twitterが、2006年3月の最初のツイートから現在までのすべての公開ツイートのインデクシングが完了し、検索できるようになったと発表した。**
- なりすまし

Facebook(1)

- 実名主義:なりすまし
- 個人とFacebookページ
- 友達になる
- Facebookページ
  - ホームページとして
  - ホームページの補完として
- 中野秀男:友達名1095(July/11/2018)
  - 2011年6月26日から
- 3名が結託されると情報が抜かれる
- 標的型攻撃の情報源

Facebook(2)

- 中野はOpinion Leader的な友達が多いので情報収集に
  - URLを拾って自分宛にメール
  - URL
- 今はFacebookやLINEの次のSNSが見えない
- 写真がスキャンされて顔認識

LINE

- 国籍は韓国
  - Twitter, Facebookはアメリカ
- LINEのアカウントの乗っ取り
  - PCで使っているとあぶない
  - 乗っ取り犯のマニュアル
- なぜ広まったのか
  - 手軽に友達に
  - スタンプ効果
- 若者はLINEでコミュニケーション、Twitterで情報収集
- 最近、トークコーナの情報がLINE社に(設定で無効に)