INSec#4 情報の防御

認証

要素技術

知識による認証

- 利用者確認情報
  - パスワード：文字列
  - パスフレーズ：1文節1句以上
  - PIN(Personal Identification Number)：暗証番号
- 固定パスワード
  - 暗号化プロトコル：SSL, IPsec
  - チャレンジ・レスポンス方式：
    サーバから送られてくる暗号鍵(チャレンジ)を受け取り、それに演算処理を組み合わせたデータ(レスポンス)を返す暗証方式→ワンタイムパスワード
- 非固定パスワード　ワンタイムパスワード
  - 生成外部デバイス・発生器
  - マトリックス認証：予め用意された文字・数字を使用
- 攻撃
  - ブルートフォースアタック
  - パスワード推測攻撃
  - 辞書攻撃
  - リプレイ攻撃
  - 盗聴
- 防御　短いパスワード＆名前に関連する文字列＆生年月日＆辞書にある単語を避ける！
- 知識による認証もトークン　token：しるし、証拠、表象
- 所持による認証を加えた多要素認証へ

所持による認証

- 利用者が所持できるデバイスにより認証
- ハードウェアトークン
  - 接触型ICカード
  - 非接触型ICカード
  - USBトークンDongle　Dongle：PCに接続する小さな装置
  - MOPASS(mobile passport)　メモリーカードにICカード機能
  - TPM(Trusted Platform Module)　ハードウェア耐タンパー性をもつセキュリティチップ-PC内に実装
- 攻撃
  - 電力解析、タイミング解析、故障利用解析
  - TEMPEST(Transient Electromagnetic Pulse Surveillance Technology)：
    コンピュータや周辺機器から発せられる微弱の電磁波から情報を盗み出す技術。
  - 盗難…紛失
- 暗号モジュール試験及び認証制度(JCMVP)　➔ http://www.ipa.go.jp/security/jcmvp/

属性による認証

- バイオメトリクス認証
  - 身体的特徴
    - 指紋　低コスト、広く普及　安価なグミから作成した人口指によりなりすまし
    - 虹彩　認証精度は高いが、高い認証コストが課題
    - 顔　認証精度の向上、耐環境性が課題
    - 血管　未知数
  - 行動的特徴
    - 音声　雑音などの耐環境性が課題
    - 署名　欧米での実績高い
- 登録と認証の２ステップ
  - 登録用テンプレート　特徴量抽出
  - 認証用テンプレート
  - 両テンプレートをマッチングし、類似度をしきい値判定
- 認証エラー
  - 他人受け入れ率：FAR(False Acceptance Rate)
  - 本人拒否率：FRR(False Rejection Rate)
- 個人情報保護

技術

ネットワークに流す利用者確認情報の暗号技術　暗号のための「鍵」

認証・セキュリティプロトコル

- L2→EAP(Extensible Authentication Protocol：拡張可能認証プロトコル)　MD5,TLS,TTLS,REAP,FAST
- L3→IPsec/IKE(Security Architecture for Internet Protocol/Internet Key Exchange protocol)
  - VPN(Virtual Private Network)を実現
  - IKEで認証、IPsecで暗号化
- L4→SSL/TLS(Secure Socket Layer / Transport Layer Security)　WWW, FTP
- L4→SSH(Secure SHell)　rlogin, telnet
- L4+…→SASL(Simple Authentication and Security Layer)　アプリケーションに組み込まれる認証プロトコル

トレードオフ(trade-off)：一方を追求すれば他方を犠牲

- 認証強度
- 認証コスト
- 利便性

オンライン手続におけるリスク評価及び電子署名・認証ガイドライン

➔ http://www.kantei.go.jp/jp/singi/it2/guide/

- 認証の保証レベル
  - 登録時のルール
  - クレデンシャルの管理ルール
  - トークンに関するルール
  - 認証プロトコルに関するルール
  - L1からL4まで

脅威

- 辞書攻撃(dictionary attack)　予測されるパスワードを集めた辞書ファイル
- リプレイ攻撃(replay attack)　ネットワークに流れる利用者確認情報をそのまま記録
- パスワード盗聴、ネットワーク盗聴
- 中間者による攻撃(man-in-the-middle attack)　中継行為-能動的攻撃
- ハイジャック攻撃(hijack attack)　認証後の通信セッション乗っ取り：セッションハイジャック

統合技術

セキュリティポリシー

- ロールベース(Role-based security policy)　役(Role)に基づき判定・許可
- ルールベース(Rule-based security policy)　全利用者にルールに基づき判定・許可

SSO(Single Sign-On)

- ユーザが一度認証を受けるだけで他の機能を利用可
- SAML(Security Assertion Markup Language)　認証情報を表現するためのXML仕様

LDAP(Lightweight Directory Access Protocol)　イントラネットでディレクトリデータベースにアクセスするためのプロトコル-認証技術

アイデンティティ管理(identity management)

ユーザのアイデンティティ情報の設定を継続的に追加・変更・削除する技術の総称
(ユーザID、ユーザ権限、ユーザプロファイル等)

デジタル署名

PKI

セキュリティプロトコル