情報ネットワークⅡ（情213）
【第14回】
演習（2）
（期末試験対策）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2018年1月25日）

演習（2）

期末試験のポイント

- 重要技術の技術名・用語とその理解
  - 特に講義資料で色文字になっている技術名・用語
- ホスト及びネットワークのセキュリティ
  - バッファオーバーフローとは？
  - セキュアOS、セキュアブートとは？
  - IDS、IPS、UTMとは？
  - NIDS、HIDS、WAFとは？
  - VPNとは？
  - ファイアウォールの構成パターンにはどのようなものがあるか？

期末試験のポイント

- ホスト及びネットワークのセキュリティ
  - ホストスキャン、ポートスキャンの手口は？
  - パスワード奪取の方法はどのようなものがある？
  - セッションハイジャックにはどのようなものがある？
  - マルウェアはタイプ別にどのようなものがあるか？
  - コンピュータウィルス対策ソフトのマルウェアを検知する仕組みにはどのようなものがあるか？

期末試験のポイント

- Webセキュリティ
  - WebブラウザがWebアプリケーションサーバーにデータを渡す2つの方法は？
  - Webセッションを管理するためのクッキーとは？
  - XSS攻撃とその対策方法は？
  - SQLインジェクション攻撃とその対策は？
  - CSRF攻撃とその対策は？

Webセキュリティ上の攻撃デモ

- バッファオーバーフロー
- XSS攻撃
- SQLインジェクション攻撃
- CSRF攻撃

By　長田研仮配生メンバー

2.3 公開鍵暗号化技術

2.3.1 RSAの仕組み

RSAの鍵生成手順

- 大きな素数 p と q をランダムに選ぶ。
- n = pq を求める（ n の長さが鍵長となる）
- (p-1)(q-1)と互いに素な正の整数 e を求める。
- ed ≡ 1(mod (p-1)(q-1))となる正の整数 d を求める。
- 公開鍵（暗号化鍵）として、e と n を公開する。
- d は秘密鍵として安全に管理する。p と q は破棄する。*重要
- 以上より、暗号化、復号は下記の通りとなる。

暗号化: $C = M^e \bmod n$ （C=暗号文、M=平文）

復号: $D = C^d \bmod n$ （D=復号文（＝平文（M））

2.3 公開鍵暗号化技術

2.3.1 RSAの仕組み

RSAの仕組みのまとめ

- ランダムに選んだ2つの素数 p, q（p≠q）とすると、n = pq を法とする世界を考える。
- 平文Mを（p-1）（q-1）と互いに素な正の整数e（公開鍵）で冪乗した値を暗号文M^e とする。
- 平文Mは{（p-1）と（q-1）の最小公倍数+1}回冪乗すると元の値に戻り、さらに{（p-1）と（q-1）の最小公倍数}回冪乗するたびに元の値に戻る性質がある。

  すなわち、整数 d を秘密鍵とすると、

  $(M^e)^d = M^{\{(p-1)(q-1)+1\}} \rightarrow ed = (p-1)(q-1)+1$

  $\therefore ed \equiv 1 \pmod{(p-1)(q-1)}$

  が成り立つ。

2.3 公開鍵暗号化技術

2.3.1 RSAの仕組み

RSAの演算の例

鍵の生成

- 2つの素数を p=3 及び q=7 とする。
- N = pq = 21　→ 21 を法とする世界を考える。
- (p-1)(q-1)と互いに素な正の整数を e=5 とする。

  ＊互いに素＝最大公約数が 1 となる数
- $ed \equiv 1 \pmod{(p-1)(q-1)}$となる正の整数をd=5 とする。
- 以上より、e=5, n=21 を公開鍵、d=5 を秘密鍵とする。

2.3 公開鍵暗号化技術

- 2.3.1 RSAの仕組み
  - RSAの演算の例
    - 暗号化
      - 平文を 2 とする。
      - $C = 2^5 \bmod 21 = 11$
    - 復号
      - $D = 11^5 \bmod 21 = 2$

2.4 鍵共有アルゴリズム

- 2.4.1 Diffie-Hellman（DH）鍵共有アルゴリズム
  - アルゴリズムの説明
    - 鍵を交換する主体をA, B とする。
    - A, B はあらかじめ素数 p とその原始根 g を交換しておく。（p, g は秘密にする必要はない）
    - 鍵の共有時は、A は乱数 x、B は乱数 y を生成し、秘密に管理する。
    - A は $n = g^x \bmod p$、Bは $m = g^y \bmod p$ を計算する。A, B は n, m を互いに交換する。（n, m は秘密にする必要はない）
    - A, B は、$K = \{m|n\}^{\{x|y\}} \bmod p = (g^{xy} \bmod p)$ を共有する暗号化鍵として使用する。
- （教科書p.53の図2.29を参照）

2.4 鍵共有アルゴリズム

- 2.4.1 Diffie-Hellman（DH）鍵共有アルゴリズム
  - DH鍵共有アルゴリズムに対するMITM攻撃
    - 主体A, B の間に攻撃者I が入り込み、I は自身が生成した n', m' をA, B に成りすましてそれぞれに転送する。
    - 問題点: 素朴なDH鍵共有アルゴリズムでは、A, B が受け取ったメッセージの真正性を確認できない。このため交換するメッセージにデジタル署名を施すなどの防御策が必要。
- （教科書p.54の図2.30を参照）

2.4 鍵共有アルゴリズム

- 原始根とは？
  - 原始根とは、素数 p を法とした場合、冪乗した値によって、素数 p より小さい値（pで割ったときの余り）がすべて得られる値のこと。
  - （例）5 を法として 3 の冪乗を計算してみる。

$3^0 \equiv 1 \pmod 5$
$3^1 \equiv 3 \pmod 5$
$3^2 \equiv 4 \pmod 5$
$3^3 \equiv 2 \pmod 5$
$3^4 \equiv 1 \pmod 5$
$3^5 \equiv 3 \pmod 5$　∴ 3 は法 5 の原始根である。

[フェルマーの小定理]
pが素数、かつ、$1 \leqq a < p$ (aは自然数) のとき、
$a^{p-1} \equiv 1 \pmod p$
が成り立つ。
なお、原始根は位数p-1の巡回群であるものとなる。

【次回予告】
第15回
期末試験

また来週！