情報セキュリティ 2019 春学期レポート課題 (1)

情報工学科 4 年 61620335 吉田一輝

1 CBC-MAC

1 ブロック分のメッセージ M に対するタグを C とする. 別のメッセージを $M' = M||(M \oplus C)$ とするとそのタグ C' は

$$\begin{aligned} C' &= E_k(M \oplus C \oplus C) \\ &= E_k(M) \\ &= C \end{aligned} \tag{1}$$

となり, メッセージ M のタグ C と一致する. このように, 異なるメッセージ長を許すともう 1 ブロック分 $M \oplus C$ を追加しこれも受信者に受理させることができてしまい, A は M を元に別のメッセージの MAC を偽造することができる.

2 RSA 暗号の計算例

2.1 d を求めよ

$$d = e^{-1} \bmod \varphi(N) \tag{2}$$
$$\Leftrightarrow ed + \varphi(N)x = 1 \tag{3}$$

となるような d と x の組を拡張ユークリッド互除法で求める. 拡張ユークリッド互除法を求める Python3 のプログラムを以下に示す.

```
1 def exgcd(m, n):
2   if n>0:
3     y,x,d = exgcd(n, m%n)
4     return x, y-m//n*x, d
5   else:
6     return 1, 0, m
7
8 d = exgcd(e, (p-1)*(q-1))[0] % ((p-1)*(q-1))
```

より, $d = 27$

2.2 平文 $M = 7$ を上記パラメータで暗号化したときの暗号文 C を求め, さらに C を復号化して M が復元されることを確認せよ

$$C = M^e \bmod N = 7^3 \bmod 55 = 13$$
$$M = C^d \bmod N = 13^{27} \bmod 55 = 7$$

3 RSA 暗号の不適切使用

同一の平文を異なる e で暗号化した暗号文が与えられるため, Common Modulus Attack が適用可能である. A さんと B さんの平文 m を暗号化した暗号文を c_A, c_B とすると, これらの暗号文は

$$c_A = m^{e_A} \bmod n \tag{4}$$
$$c_B = m^{e_B} \bmod n \tag{5}$$

と表される. 拡張ユークリッド互除法で $e_A s_A + e_B s_B = 1$ となるような s_A, s_B を見つけたとすると,

$$\begin{aligned} {c_A}^{s_A} \cdot {c_B}^{s_B} &= (m^{e_A})^{s_A} (m^{e_B})^{s_B} \bmod n \\ &= m^{e_A s_A} m^{e_B s_B} \bmod n \\ &= m^{e_A s_A + e_B s_B} \bmod n \\ &= m^1 \bmod n \\ &= m \end{aligned} \tag{6}$$

となる. よって, 平文 m は

$$\begin{aligned} m &= {c_A}^{s_A} {c_B}^{s_B} \bmod n \\ &= ({c_A}^{s_A} \bmod n \cdot {c_B}^{s_B} \bmod n) \bmod n \end{aligned} \tag{7}$$

と求めることができる.

4 RSA 署名の偽造

2 つのメッセージ m_1, m_2 に対する署名 σ_1, σ_2 を入手することで, 任意の m の署名 σ を偽造することができる.

まず乱数 r を生成し, $m_1 = m \cdot r$ を求め, m_1 の正当な署名 $\sigma_1 = m_1 \bmod n$ を入手する. 次に $m_2 = r^{-1}$ とそれに対する正当な署名 $\sigma_2 = m_2 \bmod n$ を入手する. このとき,

$$\sigma_1 \sigma_2 = m_1 m_2 \bmod n = m \bmod n \tag{8}$$

となり, これを σ とおけば与えられたメッセージ m の署名 $\sigma = m \bmod n$ を偽造できる.

5 情報セキュリティ 10 大脅威 2019 個人編

情報セキュリティ 10 大脅威選考会メンバーの投票により選出した「個人」の 10 大脅威の順位は以下の通りである.

1. クレジットカード情報の不正利用
2. フィッシングによる個人情報等の詐取
3. 不正アプリによるスマートフォン利用者への被害
4. メール等を使った脅迫・詐欺の手口による金銭的要求
5. ネット上の誹謗・中傷・デマ
6. 偽警告によるインターネット詐欺
7. インターネットバンキングの不正利用
8. インターネットサービスへの不正ログイン
9. ランサムウェアによる被害
10. IoT 機器の不適切な管理

5.1 クレジットカード情報の不正利用

メールの添付ファイルを利用してウィルスに感染させてクレジットカード情報を窃取したり, 偽のサイトに情報を入力させてクレジットカード情報を窃取する (フィッシング詐欺) 手法が存在する. 抜き取ったクレジットカード情報を用いてショッピングサイトで不正に購入する手口が報告されている.

この攻撃に対する早期発見としては, 利用者側においてはクレジットカードの利用履歴の確認や, カード利用時のメール通知機能等使用することによって不審なカード利用に気づくことができる. また現在では, カード会社が普段の購入傾向と著しく異なったカード利用が検出された場合, カード利用者に電話確認を行なったり一旦カードの利用を停止させることが行われている. そもそもカード情報を抜き取られないようにするため, 怪しげなメールの添付ファイルは開かない, クレジットカード情報を入力するように誘導させるメールに載っているフィッシングサイトにはカード情報を入力しない, 海外旅行の際にはカード情報のスキミングに気をつけるといったことが挙げられる.

5.2 フィッシングによる個人情報等の詐取

実在する企業を装い, フィッシングサイトに誘導して利用者が入力した情報を窃取する攻撃がある. 最近個人的によく目にするのが Apple を装ったフィッシング詐欺で, Apple アカウントが不正利用されているからログインしてアカウントを復帰させる必要があるとの文面でメールを送りつけ, フィッシングサイトの URL にアクセスさせて Apple ID を抜き出す手口がある. この攻撃が成功すると, Apple Pay 等のサービスから商品を不正に購入することができる.

被害の予防策としては, 企業が直接ログインを促すメールを送信することは少ないので, むやみに受信メールの URL を開かないことが挙げられる. 被害の早期発見には, アカウントの記録を確認したり, アカウントに紐づけられているクレジットカード等の履歴を確認することが有効だろう.

5.3 不正アプリによるスマートフォン利用者への被害

正規のアプリケーションを模して作られた不正なアプリケーションをスマートフォンにインストールしてしまうことで, 不正アプリを通じて個人情報を抜き取られてしまう攻撃手口が存在する. 不正なアプリを利用した個人情報への攻撃は多数考案されており, 例えば GPS に不正にアクセスすることで自宅や勤務地を特定す

ることや, マイクに不正にアクセスすることで盗聴を行うことができる.

これらの対策としては, Android は公式マーケット以外からもアプリケーションがインストールすることができるがそれを行わず, 必ず Google や Apple の審査を通ったものだけを利用するように心がけることが重要である. また, 公式マーケットからインストールされたものでも, 必要のないと思われるセンサへのアクセス権を要求するアプリケーションには注意が必要である.

5.4 メール等を使った脅迫・詐欺の手口による金銭的要求

アダルトサイトの閲覧料金が未納であるので今すぐ支払え, といったものやいついつまでにお金を支払わなければ裁判を起こす等の脅迫を行なって金銭を要求する詐欺・脅迫手口がある. アダルトサイトの閲覧等は, 被攻撃者が他人に相談しにくい事柄であるため金銭を支払ってしまう可能性が高い. また, 脅迫文内にメール受信者のパスワードを記載していることもあり, ハッキングされていると信じてしまいがちである.

メール本文の日本語が怪しかったりした場合は気をつけるべきだろう. メール本文内にパスワードの記載があったとしても, 不正な金銭要求には応じないよう心がけることが重要だ.

5.5 ネット上の誹謗・中傷・デマ

SNS 等で他人を誹謗・中傷したり, 脅迫・犯罪予告を書き込み事件になる. また, 嘘情報やフェイクニュースが拡散されてしまう. 東日本大震災時には, ライオンが動物園から抜け出したり, ヨウ素を窃取すると放射線被曝を抑えることができるとのデマが拡散された. ネットの情報を鵜呑みにしてしまうネットリテラシーの欠如や, 個人の匿名性が確保されており誰でも情報の発信者になれるという現代の状況をよく表している.

この対策として, 個人がネットの情報を全て検討するのは現実的に不可能なので, 一人一人がネットの情報を吟味できるような, また不満やストレスを他人への攻撃に方向付けないようなネットリテラシーを育むことが必要である. 自分が誹謗中傷の被害にあった場合, 一人で抱え込まずに公的相談機関に相談すると良い.

5.6 偽警告によるインターネット詐欺

インターネット閲覧中に, ウィルスに感染しました！等不安を煽り, 不要なソフトウェアのインストールやサポート契約を結ばせる攻撃手口がある. アダルトサイトを見ている際に多いが, 警告画面をポップアップで表示させ契約するまで繰り返し不安を煽ることが多い.

この対策は, 使用しているブラウザの種類にもよるが, Google 検索でポップアップを削除する方法を調べれば簡単に出てくるので, 不安に駆られずに冷静に対処することが必要である. そのような警告はほぼ全て偽物であるため, 落ち着いてブラウザを消せばよい.

5.7 インターネットバンキングの不正利用

ウィルスに感染させてインターネットバンキングの ID やパスワードを抜き出したり, フィッシングサイトを利用してインターネットバンキングのアカウントを詐取することで不正送金を行う攻撃手口である.

対応策は, フィッシングによる個人情報窃取と同様, メールで誘導されるフィッシングサイトに注意することが考えられる.

5.8　インターネットサービスへの不正ログイン

ウィルスに感染させインターネットサービスの ID とパスワードを入手する攻撃や, 利用者の名前や誕生日等の利用者が使いそうなパスワードを推測して不正ログインを試みる攻撃, なんらかの手段で手に入れた同じ利用者の他のサービスの ID とパスワードを手に入れてそれを使い回す攻撃がある.

これらの攻撃への対策として, パスワードを簡単なものにしないことが考えられる. パスワードは短すぎず, ある程度複雑なものにすることでパスワード推測攻撃を行いにくくすることができる. また, 利用頻度が低いサービスや不要なサービスのアカウントを削除することで, パスワード管理を楽にすることができ, そのような情報が流出する危険性を抑えることができる.

5.9　ランサムウェアによる被害

PC やスマートフォンのファイル暗号化や画面ロックを行い, その解除と引き換えに金銭を要求するウィルスが流行ったことがあった. Wanna Cry というランサムウェアは, 感染すると Windows 上のファイルが暗号化され Wanna Cry?と表示され, 暗号化の解除にはビットコインを送金することが要求されている. このランサムウェアは工場や病院のパソコンに感染し, 実際に手術が遅れてしまったり重大な損害を被った.

Wanna Cry に代表されるランサムウェアは, パソコンのオペレーティングシステムの脆弱性を突いたものが多い. Microsoft は Wanna Cry が流行する数ヶ月前にオペレーティングシステムのアップデートを行っていたが, Wanna Cry の被害にあった人はみなオペレーティングシステムのアップデートをしていなかった. 常に最新のオペレーティングシステムにアップデートしておくことでこうした攻撃を防ぐことができる.

5.10　IoT 機器の不適切な管理

これからの時代は Society5.0 が目指されていることもあり, 一般家庭でも IoT 機器が存在するようになるが, パスワードの設定や管理が不十分な IoT 機器に不正アクセスされ情報の盗み見などの被害が発生する. 初期パスワードのままにされていた監視カメラへの不正アクセスや, IoT 機器を用いた DDoS 攻撃が行われた.

企業はその暗号化の取り扱い等に十分注意を払う必要がある. IoT 機器が将来的にどれくらいの時代まで用いられるかを考えて適切なセキュリティを構築することが重要だ. 個人ができる対策としては, IoT 機器を買ったらパスワードを変更すること, また外部からのアクセスポートを制限することで外部からの攻撃をできるだけ通さないようにすることが必要である.