情報セキュリティ 2003年度期末試験

授業科目名 情報セキュリティ　担当者名 小林吉純　対象学生 IS科3年A組・B組 II科3年A組・B組　参照・使用許可物等 なし

1. PKIとは何かを提供機能を含め、説明せよ。また、パスワードやバイオメトリクスによる認証に比べ、PKIによる認証が優れている点を箇条書きで5個記述せよ。

①PKIとは何か

PKIとはPublic Key Infrastructureの略称で、公開鍵暗号方式をベースに共通鍵暗号方式を組み合わせ、通信相手や文書作成者の認証、文書の完全性チェック、文書の秘匿性保証などの情報セキュリティに関する機能を提供する情報基盤のことである。

提供機能の記述漏れなどは減点

②PKIによる認証が優れている点

・個人の秘密情報を預かる必要がなく、特定システムに依存しない広域性を有する。
・他人の秘密情報を預かる必要がないので、他の認証サーバとは異なり、不正侵入等により、他人の秘密情報を盗まれる危険がない。
・秘密情報を送信する必要がなく、ネットワークでの認証に効果的である。
・パスワードのように記憶に頼ることがなく、なりすましの危険が格段に少ない。
・パスワードに比べると、秘密情報(秘密鍵)の解読が極めて困難である。
・バイオメトリクス認証に比べ、特別な装置が不要で、導入に抵抗がない。
・バイオメトリクス認証では認証の確実性を100%にすることは困難であるが、PKIではそれが可能である。

これらのうち、5個

2. ディジタル署名、メッセージ認証(メッセージ認証コードMACを用いた方式)それぞれの方式に関して、ディジタル署名、MACそれぞれの作成、検証の観点から説明せよ。

ディジタル署名とは文書に対するハッシュ値を公開鍵暗号方式における秘密鍵で暗号化したものであり、文書と一体で送信または保管される。署名の検証はディジタル署名を署名時の秘密鍵に対応する公開鍵で復号し、その結果を文書のハッシュ値と比較することにより行う。これにより、文書の完全性チェックと文書作成者の認証を行える。

メッセージ認証では送受信者間で秘密情報を共有しておき、送信側はメッセージ(文書)と秘密情報を連結した結果のハッシュ値を取り、それをメッセージ認証コード(MAC)とする。送信側はメッセージとMACを受信側に送信する。受信側では受信したメッセージと秘密情報を連結した結果のハッシュ値を取り、それと受信したMACを比較することにより、メッセージの完全性チェックと送信側の認証を行う。

作成、検証のうち、一方しかない解答は減点

3. 攻撃対象ホストでの通信サービスの稼動状況を調べるため、ポートスキャンという手法が用いられる。①ポートスキャンの定義を述べた後、②TCPの3ウェイハンドシェークを用いたポートスキャンの方法を説明せよ。

①ポートスキャンの定義

通信サービスのプロトコルにはポート番号が割り当てられている。ポートスキャンとはポート番号を指定したTCPやUDPのパケットを攻撃対象ホストに送信し、その応答に基づき、通信サービスの稼動状況(ポートの開き状況)を調べる手法である。

②TCPポートスキャンの方法

TCPは3ウェイハンドシェークにより開始される。この時、SYNパケットに対し、SYN/ACKパケットが返却されてくれば、正常応答であり、ポートは開きと判断できる。これに対し、RST/ACKパケットが返却されてくれば、異常応答であり、ポートは閉じていることになる。

SYN、SYN/ACK、RST/ACKの記述が正しくない場合は減点

4. 相異なる2つの素数をp=3、q=17とする。
(1)この時、RSA暗号の公開鍵e、nのうち、e=5として問題ないことを示し、残りのnを求めよ。
(2)また、秘密鍵dをユークリッドの互助法に基づき計算せよ。
(3)更に、平文M=42とした場合の暗号文を求めよ。
何れも、計算過程を記述すること。

参考
(1) k=LCM(p-1,q-1)とおくと、eは条件(k,e)=1を満たす
(2) ed≡1 mod k

(1)
k=LCM(p-1,q-1)=LCM(3-1,17-1)=LCM(2,16)=16
e=5 は条件(k,e)=1を満たすので、問題なし。
n=pq=3×17=51
従って、公開鍵はn=51、e=5

(2)
ed≡1 mod kより、5d≡1 mod 16 ①
恒等的に成り立つ式 16d≡0 mod 16 ②
5と16にユークリッドの互助法を適用すると
16=3×5+1
5=5×1
従って、
①×3 -15d≡3 mod 16 ③
②−③ d≡−3 mod 16 ④
余りを正の整数にするとd≡13 mod 16
従って、秘密鍵d=13

(3)
公開鍵n=51、e=5による暗号化
$C \equiv M^e \bmod n = 42^5 \bmod 51$
$42^5 \equiv ((-9)^2)^2 \times (-9) = 81^2 \times (-9) \equiv (-21)^2 \times (-9) = 441 \times (-9) \equiv (-18) \times (-9) = 162 \equiv 9$
即ち、暗号文C=9

5. サーバは自身の秘密鍵Ss、公開鍵Ps及び公開鍵証明書を所有している。サーバでクライアント用の秘密鍵Sc、公開鍵Pcを作成したとして、この秘密鍵Scを安全にクライアントへ送信する場合の手順(どちらで何の鍵を生成するか、どの鍵で暗号化した何をどちらからどちらへ送信するか、どちらでどの鍵を使用して何を復号するか、など)を箇条書きで記述せよ。但し、サーバ、クライアント共に、共通鍵生成プログラム、共通鍵暗号プログラム、公開鍵暗号プログラムが実装されているが、クライアントには公開鍵／秘密鍵の生成機能はないものとする。

・サーバからクライアントに公開鍵Psが格納された公開鍵証明書を送信
・クライアントで、共通鍵Cを生成
・クライアントで、公開鍵証明書内の公開鍵Psで共通鍵Cを暗号化し、サーバへ送信
・サーバで、秘密鍵Ssで受信データを復号し、共通鍵Cを取り出す
・サーバで、共通鍵Cで秘密鍵Scを暗号化し、クライアントへ送信
・クライアントで、共通鍵Cで受信データを復号し、秘密鍵Scを取り出す

「公開鍵証明書の送信」の記述漏れが多かった

5. 共通鍵暗号やハッシュを用いても、秘密情報を生の形で通信路に流すことなく、認証が行える。共通鍵暗号またはハッシュを用いて、相手認証を行う手順を箇条書きで記述せよ(共通鍵暗号またはハッシュの何れか一方の記述でよい)。但し、認証側、被認証側双方で同一共通鍵または共有秘密を保持していることを前提とする。

(a)共通鍵暗号
・認証側で乱数(チャレンジ)を生成し、被認証側へ送信
・被認証側でチャレンジを共通鍵で暗号化し、それを認証側へ送信
・認証側で受信データを共通鍵で復号し元のチャレンジと比較
・比較結果が一致であれば、認証OKと判断

−共通暗号または−ハッシュを用いてであり、両方の使用は不可
−共通鍵または共有秘密−であり、両方の使用は不可

(b)ハッシュ
・認証側で乱数(チャレンジ)を生成し、被認証側へ送信
・被認証側で共有秘密とチャレンジを連結し、そのハッシュを取り、ハッシュ値を認証側へ送信
・認証側でも共有秘密とチャレンジを連結し、そのハッシュを取り、受信データと比較
・比較結果が一致であれば、認証OKと判断