Computer and network security. Final exam 09-07-2012. Time: 120 minutes

1. Digital signature

Answer the following questions, where x denotes the private key of the signer.

- With reference to a generic digital signature scheme, why defining the signature as $Enc_x(H(M))$, rather than $Enc_x(M)$? Discuss.
- Illustrate the PKCS standard for digital signature using RSA and discuss the different fields of the signed record.
- Suppose Alice signs through DSA l documents M_1, M_2, …, M_l using her private key x, but she uses only l-1 different values for k (one value is used twice). Can an attacker gain advantage from that?

2. Average guessing game

A, B and C play the following game. Each of them secretly chooses an integer in [0,N]; let such numbers be, respectively, a, b and c. Then the average $z = (a+b+c)/3$ is computed. The winner of the game is the player who chose the integer closest to z. The players use the following protocol.

[A chooses a and nonce r_a, then computes $x_a = r_a(a)$]
A → B: x_a
[B chooses b e un nonce r_b, then computes $x_b = r_b(b)$]
B → C: x_a, x_b
[C chooses c]
C → A: x_b, c
A → B: r_a, c
[now B knows a, b and c]
B → C: r_a, r_b
[now C knows a, b and c]
C → A: r_b
[now A knows a, b and c]

- Discuss the robustness of the protocol with respect to possible fraudulent behaviors from A, B and/or C.
- Modify the protocol for fixing the detected problems.

3. Authentication based on public key

- Describe the original Needham-Schroeder scheme, its vulnerability and its fixing.
- Describe a one-way authentication scheme based on X509 certificates and discuss what guarantees it ensures.

4. Block ciphers modes of operation

- Define the practical scenario where block ciphers modes of operation occur and the following modes: ECB, CBC and OFB.
- Compare the three modes in terms of: robustness to passive attacks, parallelizability, error propagation and possible similarity to stream ciphering.

5. Briefly answer the following (at most 8 lines & 1 picture per question – using more space does not increase the quality)

- Discuss how to introduce security mechanisms on IP and on TCP. What differences? What application scenarios?
- Firewalls: compare stateless packet filtering to session filtering.

Sicurezza nelle reti e nei sistemi informatici. Esame del 09-07-2012. Tempo: 120 minuti

1. Firma digitale e schema di firma di El-Gamal

Rispondere alle seguenti domande, in cui x denota la chiave privata del firmatario.

- Con riferimento a uno schema generico di firma, perché è opportuno definire la firma digitale come $Enc_x(H(M))$, piuttosto che come $Enc_x(M)$? Discutere.
- Descrivere le procedure di firma e di verifica secondo lo schema di El-Gamal (denotare con k il valore casuale generato a ogni firma).
- Supporre che Alice firmi l documenti M_1, M_2, …, M_l usando la sua chiave privata x, ma utilizzando solamente l-1 valori differenti di k (un valore viene usato due volte). Come può un attaccante sfruttare la circostanza?

2. Gioco "indovina la media"

A, B e C giocano a "indovina la media". Il gioco consiste nello scegliere segretamente un intero in [0, N] (un intero per ciascun giocatore) e calcolare la media dei valori scelti. Il giocatore che ha scelto l'intero più vicino alla media vince. Viene usato il seguente protocollo.

[A sceglie a e un nonce r_a, quindi calcola $x_a = r_a(a)$]
A → B: x_a
[B sceglie b and nonce r_b, quindi calcola $x_b = r_b(b)$]
B → C: x_a, x_b
[C sceglie c]
C → A: x_b, c
A → B: r_a, c
[ora B conosce a, b e c]
B → C: r_a, r_b
[ora C conosce a, b e c]
C → A: r_b
[ora A conosce a, b e c]

- Discutere la robustezza del protocollo rispetto a possibili comportamenti fraudolenti da parte di A, B e/o C.
- Modificare il protocollo per rimuovere le debolezze individuate.

3. Autenticazione basata su chiave pubblica

- Descrivere lo schema originale di Needham-Schroeder, la sua vulnerabilità e la modifica che si rende necessaria.
- Descrivere uno schema di autenticazione a una via (one-way) basato su certificati X509 e discutere le garanzie da esso assicurate.

4. Modi di operazione di cifrari a blocchi

- Definire lo scenario pratico in cui si utilizzano i modi di operazione dei cifrari a blocchi e descrivere i modi ECB, CBC e OFB.
- Confrontare i tre modi in termini di: robustezza contro attacchi passivi, parallelizzabilità, propagazione degli errori ed eventuali similarità con i cifrari a flusso.

5. Rispondere brevemente alle seguenti domande (max 8 linee e una figura per domanda – l'utilizzo di spazio aggiuntivo non migliora la risposta)

- Discutere l'introduzione di strumenti di sicurezza su IP e su TCP. Quali differenze, quali scenari?
- Firewall: confrontare filtraggio di pacchetti stateless con filtraggio basato su sessione.