CS 161 Computer Security
Fall 2006 Joseph/Tygar

MT 1 Solutions

Problem 1. [Definitions] (16 points)

Please give a *short* (one sentence) definition for each of the following terms. (2 points apiece)

(a) (Cryptanalysis) Brute-force attack

Attacking a cipher by trying all possible keys in the keyspace until the correct one is found.

(b) (Cryptanalysis) Known-plaintext attack

An attack in which one or more plaintext/ciphertext pairs are known.

(c) (Cryptanalysis) Chosen-plaintext attack

An attack in which the attacker may know the ciphertext for one or more plaintexts of his/her choice.

(d) (Access control) Authorization

The right of a subject to access an object. [Also: Granting a subject access to an object/resource.]

(e) (Access control) Authentication

Verifying the identity of a subject or of a message's source.

(f) (Message protocols) Nonce

A random value, timestamp, or counter added to a message to make it unique (and guarantee freshness).

(g) (Firewalls) Security policy

The policy specifying which network services should be available and what types of access should be denied. [Not to be confused with a firewall ruleset, which is the mechanism that implements the policy.]

(h) (Firewalls) Reference monitor

A component that mediates access to the network and is always invoked, verifiable, and tamper-resistant.

Problem 2. [Cryptography] (28 points)

(a) (4 points) What are revocation lists for public-key certificates?

Lists of revoked public-key certificates.

(b) (8 points) One way to handle revocation is to put an expiration date in a public key certificate. When the expiration date is reached, the certificate is no longer valid and will not be renewed. What are the disadvantages of this approach?

No way to revoke before expiration date.

(c) (8 points) A second way to handle revocation is to maintain a list of "bad public-key certificates" at a central repository that is heavily protected from attack. Assuming that it is possible to protect the repository from attack, what are the disadvantages of this approach?

Requires an online repository; may have issues with availability, scaling.

(d) (8 points) A third way to handle revocation is to broadcast a secure message to all parties alerting them that a particular public key certificate has been compromised. What are the disadvantages of this approach?

Parties need to be online to receive broadcasts.

Problem 3. [Shamir Secret Sharing] (28 points)

(a) (14 points) Let us review how the Shamir secret sharing system works. The creator of a secret uses a function $f(x) = x^n + a_{q-1}x^{n-1} + \ldots + a_1 x + a_0 \mod p$. What is the secret? What are the secret shares? The modulus p must be larger than the secret; what other restrictions are there on p? How are the shares created? How is the secret reconstructed?

Let p be a large prime, a_0 be the secret, and $a_1, \ldots, a_{q-1}$ be random values modulo p.

Then the secret shares are $\langle 1, f(1)\rangle$, $\langle 2, f(2)\rangle$, $\ldots \langle t, f(t)\rangle$. With q such secret share values, we are solving q linear equations over q unknowns modulo p (called lagrangian interpolation). We solve and find a_0.

(b) (7 points) One problem with the Shamir secret sharing scheme is that if one of the secret holders is compromised, s/he may provide a bad secret share during reconstruction. In other words, if s/he holds secret s_i, s/he may provide a value different from s_i. Why does this cause a problem for secret sharing?

With bad secret shares we will have incorrect reconstruction of the secret.

(c) (7 points) To solve this problem with secret sharing, we may try adding a digital signature. There are two approaches we could use: (i) the secret-share generator could add the digital signature to the secret originally and then generate the secret shares from the signed secret. (ii) the secret-share generator could take the secret and break it into shares, but before distributing the shares, add a digital signature to each share. Compare the advantages and disadvantages of each approach.

(i) is faster (only one signature) but does not identify the bad share.

(ii) requires more signatures and verifications but makes bad shares obvious.

Problem 4. [Firewalls] (28 points)

The following diagram shows the architecture for your company's network and connection to the internet.

Your company is installing a packet filter firewall. Here is the proposed security policy for the firewall:

1. By default, block all inbound connections.
2. Allow all inbound TCP connections to SMTP on mail server.
3. Allow all inbound TCP connections to HTTP and HTTPS on web server.
4. Allow all inbound TCP connections to SSH on SSH server.
5. Allow all outbound connections.
6. Telnet access should not be allowed (because it sends passwords in cleartext).

(a) (12 points) Using the syntax from lecture (examples above), write the firewall ruleset for your company's firewall. For each rule, give a brief description of its purpose.

Square brackets around /in or /out mean they may be included but are not strictly necessary.

(i) `allow tcp *:*[/out] -> 1.2.3.5:25[/in]` (allow SMTP)
(ii) `allow tcp *:*[/out] -> 1.2.3.4:80[/in]` (allow HTTP)
(iii) `allow tcp *:*[/out] -> 1.2.3.4:443[/in]` (allow HTTPS)
(iv) `allow tcp *:*[/out] -> 1.2.3.3:22[/in]` (allow SSH)
(v) `drop  tcp *:*[/in]  -> *:23[/out]` (drop telnet)
(vi) `allow tcp *:*/in  -> *:*/out` (allow all outbound)
(vii) `allow tcp *:*/out  -> *:*/in  (if ACK bit set)` (allow TCP responses)
(viii) `drop  *  *:*[/out] -> *:*[/in]` (default deny)

Note that the default deny rule will stop incoming telnet connections.

(b) (8 points) Hackers target your company's network with repeated requests for large images on your company's webserver. The hackers machines are on the `20.1.21.x` subnet. How could you change your firewall ruleset to block these attacks?

Add the rule:

```
drop  tcp 20.1.21.*:*[/out] -> *:*[/in]
```

or:

```
drop  tcp 20.1.21.0/24:*[/out] -> *:*[/in]
```

as the FIRST rule in the ruleset.

(c) (8 points) Employees start downloading lots of movie trailers from the new Pear SlowTime website at `4.3.2.1:80`. How could you change your firewall rules to stop employees from accessing the website?

Add the rule:

```
drop  tcp *:*[/in] -> 4.3.2.1:80[/out]
```

before rule

```
allow tcp *:*[/in] -> *:*[/out]
```