Security Chapter 4

[1] authentication

Something the user knows (Passwords, Cryptography
Something the user has (Memory token, Smart token
Something the user is (biometric

[2] what is meant by authentication, and what security goals it affect

Authentication is the process of identifying the identity of the user.
Authentication mechanisms to confirm a user's identity.

1. **Something the user knows**: Passwords, PIN numbers, passphrases, a secret handshake, and mother's maiden name are examples of what a user may know.
2. **Something the user has.** Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.
3. **Something the user is.** These authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture).

[3] problems with passwords

- Guessing or finding the password
- Giving passwords away, users may share the password
- Electronic monitoring.
- Accessing the password file
- Password used as access control

[4] Tokens

Memory token store, but do not process, information. A special reading / writing device control reading / writing of data.
A common application is **automatic teller machine (ATM)**

Benefits:

1. Memory tokens used with PINs provide significantly more secure than passwords
2. Memory cards are inexpensive
3. The hacker must have a valid token and the corresponding PIN.

Problems:

1. most of problems associated with them relate to cost, administration, token loss.
2. Most techniques of increasing security relate to protection of PIN.
3. Require a special reader.
4. Token loss
5. User dissatisfaction.

Smart token
It expands functionality of the memory token by incorporating one or more interated circuits into the token itself.

Kerberos: The Network Authentication Protocol