Models Annex: Cryptographic Models in simple situation (example) (2)
- Standard model: *authentication by password* (2)
- Random Oracle model: *authentication by password* (4)
- Ideal Cipher model: *authentication by password* (6)
- Universal Composability model: *authentication by password* (8)

Models Annex:
Cryptographic Models in simple situation (example)

Standard model: *authentication by password*

Situation

- a user chooses a password wisely
- the system stores password hashes using SHA-256
- the administrators of the authentication system are honest and competent

...Standard model: password authentication (cont.)

Assumptions

- real algorithm is used: SHA-256 hashing
- user chooses strong passwords (i.e. long and random-looking)
- attacker:
  - might steal the hashed password's database
  - uses up-to-date software and hardware
  - has lots of time but does not live forever
  - cannot break SHA-256

Security Claim

- "*No clever, resourceful attacker can recover a password, as long as SHA-256 remains unbroken and the system's administrators remain honest.*"

Random Oracle model: *authentication by password*

Situation

- a user chooses a password wisely
- the system stores password hashes using a perfect random function
- the administrators of the authentication system are honest and competent

...Random Oracle model: password authentication (cont.)

Assumptions

- ideal algorithm is used: perfect random function
- user chooses strong passwords, perhaps by questioning a Random Oracle (i.e. long and random)
- attacker:
  - might steal the hashed password's database
  - uses up-to-date software and hardware
  - has lots of time but does not live forever
  - can, of course, query the same Random Oracle has long as he/she wants

Security Claim

- "*No clever, resourceful attacker can recover a password, as long as the system's administrators remain honest*."

Ideal Cipher model: *authentication by password*

Situation

- a user chooses a password wisely
- the system stores password cipher using a perfect cipher function with a secret key
- the administrators of the authentication system are honest and competent

...Ideal Cipher model: password authentication (cont.)

Assumptions

- ideal block cipher algorithm is used: completely random permutation[1]
- user chooses strong passwords (i.e. long and random-looking)
- attacker:
  - might steal the database with the enciphered passwords
  - uses up-to-date software and hardware
  - has lots of time but does not live forever
  - can, of course, try ciphering any password he wants with known cipher function, but cannot break it, nor knows the secret key used by authentication system

Security Claim

- "*No clever, resourceful attacker can recover a password, as long as the system's administrators remain honest*."

1 Every input block is mapped to a random output block.

Universal Composability model: *authentication by password*

Situation

- a user chooses a password wisely
- the system stores password hashes using an yet unbroken hashing function
- the managers of the authentication system are honest and competent
- the authentication system is running at the same time as many other systems

...Universal Composability model: password authentication (cont.)

Assumptions

- hashing algorithm is yet unbroken
- user:
  - chooses strong passwords (i.e. long and random-looking)
  - concurrently uses other computer systems (e.g. web browser, word processor...)
- attacker:
  - might steal the hashed password's database
  - uses up-to-date software and hardware
  - has lots of time but does not live forever
  - can interact with other systems, look for vulnerabilities and combine info

Security Claim

- "*No clever, resourceful attacker can recover a password, as long as all used concurrent systems remain secure and the system's administrators remain honest*."