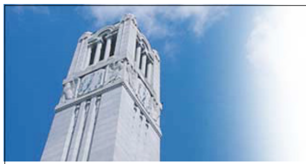


NC STATE UNIVERSITY Computer Science

CSC 474
Information Systems Security

Topic 3.2: User Authentication

User Authentication

- What the user knows
  - passwords, personal information
- What the user possesses
  - a physical key, a ticket, a passport, a token, a smart card
- What the user is (biometrics)
  - fingerprints, voiceprint, signature dynamics

Passwords

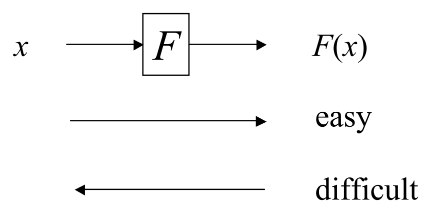
- Most commonly used method.

Storing User Passwords

- Directly Store the Passwords?
  - Not a good idea!
  - High risk
    - Anyone who captures the password database could impersonate all the users.
    - The password database would be very attractive to hackers.

One-Way Hash Function

- One-way hash function F
  - $F(x)$ is easy to compute
  - From $F(x)$, x is difficult to compute
  - Example: $F(x) = g^x \bmod p$, where p is a large prime number and g is a primitive root of p.



Storing Passwords

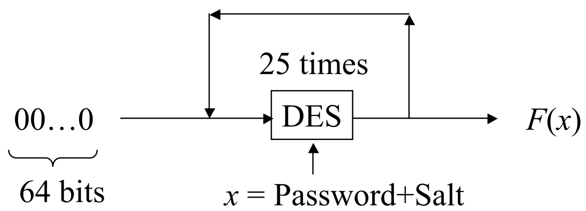
- For each user, system stores

  (*user name*, F(*password*))

  in a password file, where F is a one-way hash function
- When a user enters the password, system computes F(*password*); a match provides proof of identity

What is *F*?

- crypt Algorithm (Unix)
  - Designed by Bob Morris and Ken Thompson
  - Use Data Encryption Standard (DES) encryption algorithm
  - User password and salt is used as the encryption key to encrypt a 64-bit block of zeros
  - This process is repeated 25 times



Choice of Passwords

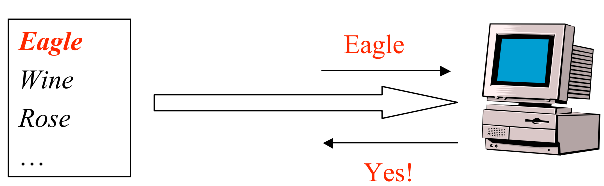
- Suppose passwords can be from 1 to 9 characters in length
- Possible choices for passwords = $26^1 + 26^2 + ... + 26^9 = 5 * 10^{12}$
- At the rate of 1 password per millisecond, it will take on the order of 150 years to test all passwords

Choice of Passwords (Cont'd)

- However, we don't need to try all possible passwords, only the probable passwords
- In a Bell Labs study (Morris & Thompson 1979), 3,289 passwords were examined
  - 15 single ASCII characters, 72 two ASCII characters, 464 three ASCII characters, 477 four alphanumeric character, 706 five letters(all lower or all upper case), 605 six letters all lower case, 492 weak passwords (dictionary words spelled backwards, first names, surnames, etc.)
  - Summary: 2,831 passwords (86% of the sample) were weak, i.e., they were either too easily predictable or too short

Dictionary Attacks

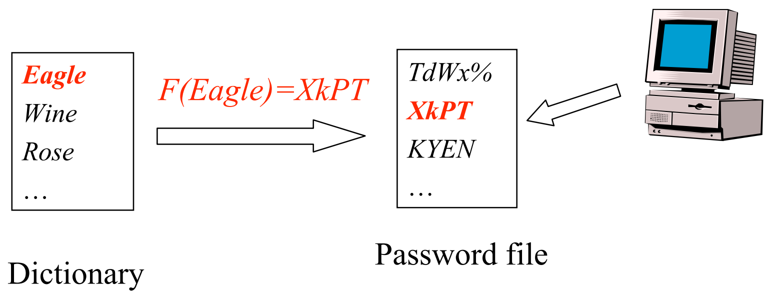
- Attack 1:
  - Create a dictionary of common words and names and their simple transformations
  - Use these to guess the password



Dictionary

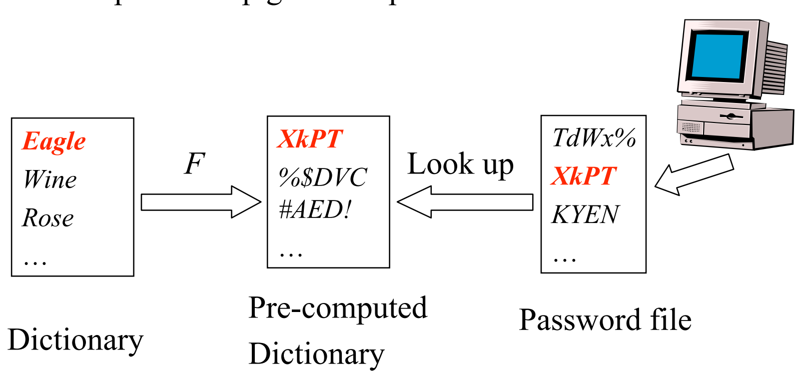
Dictionary Attacks (Cont'd)

- Attack 2:
  - Usually *F* is public and so is the password file
    - In Unix, *F* is crypt, and the password file is /etc/passwd.
  - Compute *F*(*word*) for each word in the dictionary
  - A match gives the password



Dictionary Attacks (Cont'd)

- Attack 3:
  - To speed up search, pre-compute *F*(dictionary)
  - A simple look up gives the password

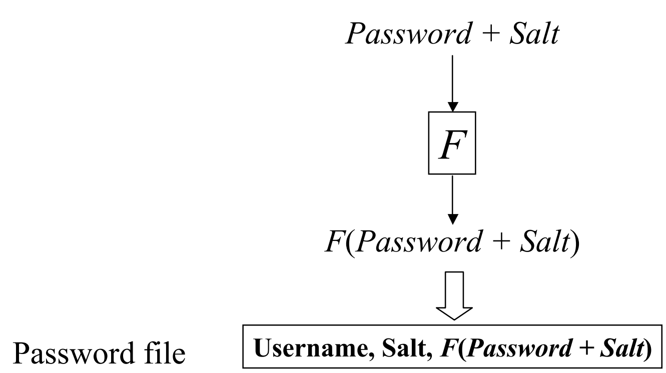


Password Salt

- To make the dictionary attack a bit more difficult
- Salt is a 12-bit number between 0 and 4095
- Derived from the system clock and the process identifier

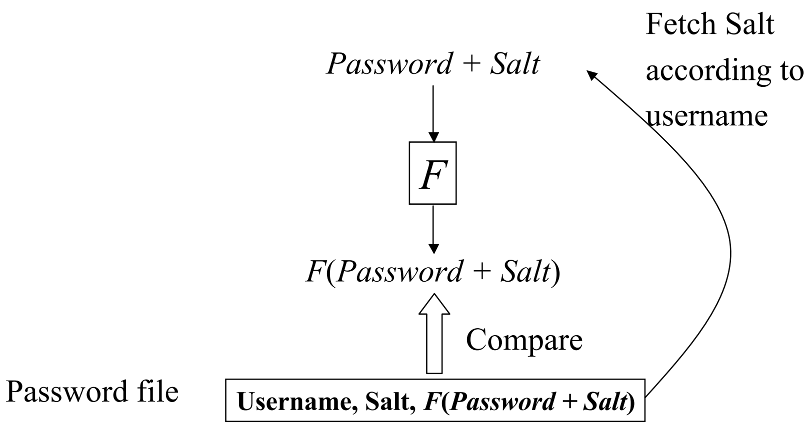
Password Salt (Cont'd)

- Storing the passwords



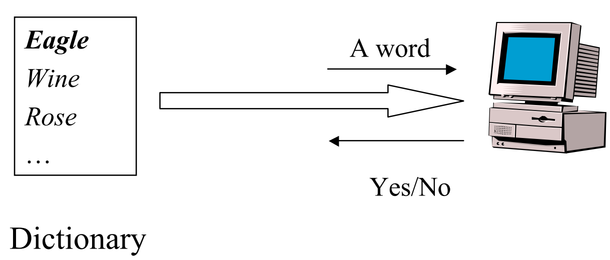
Password Salt (Cont'd)

- Verifying the passwords



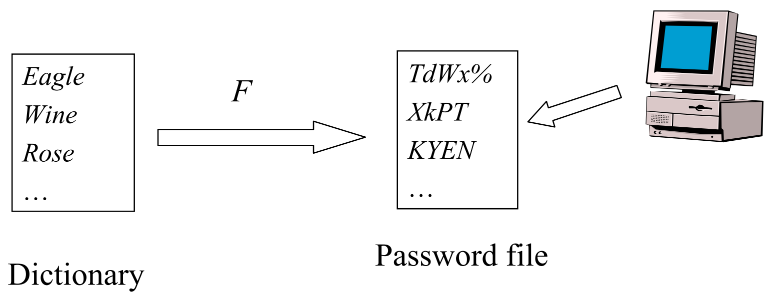
Does Password Salt Help?

- Attack 1?
  - Without Salt
  - With Salt



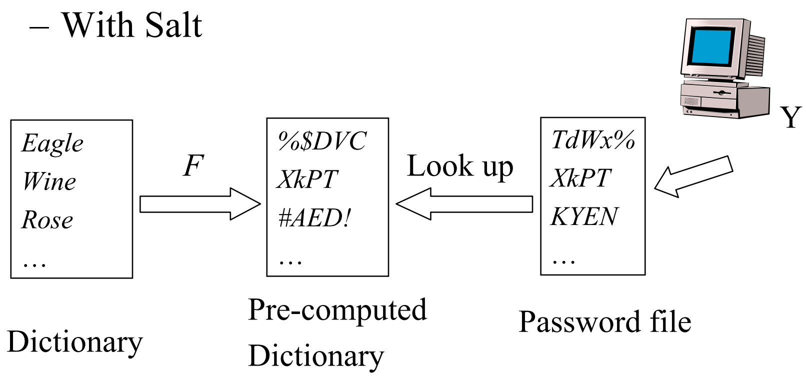
Does Password Salt Help?

- Attack 2?
  - Without Salt
  - With Salt



Does Password Salt Help?

- Attack 3?
  - Without Salt
  - With Salt



Password Management Policy and Procedure

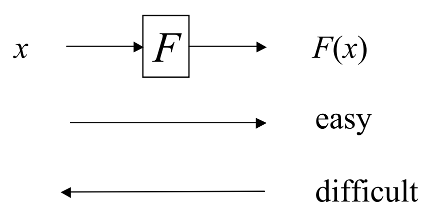
- Educate users to make better choices
  - Does not work if the user population is large or novice
- Define rules for good password selection and ask users to follow them
  - Rules serve as guideline for attackers
- Ask or force users to change their passwords periodically
- Force users to use machine generated passwords
  - Random passwords are difficult to memorize; also password generator may become known to the attacker through analysis
- Actively attempt to break users' passwords; force users to change those that are broken
  - Attacker may have better dictionary
- Screen password choices; if a choice is weak, force users to make a different choice

One-time Passwords

- Use the password exactly once!

Lamport's Scheme (S/Key)

- Take advantage of One-Way function
- One-way hash function F
  - F(x) is easy to compute
  - From F(x), x is difficult to compute

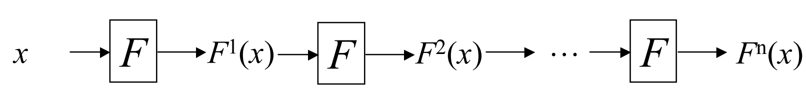


S/Key (Cont'd)

- Pre-computation

The System

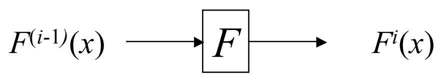
1. Randomly generate x
2. Compute the following



3. Save (*username*, $F^n(x)$), and give x to the user.

S/Key (Cont'd)

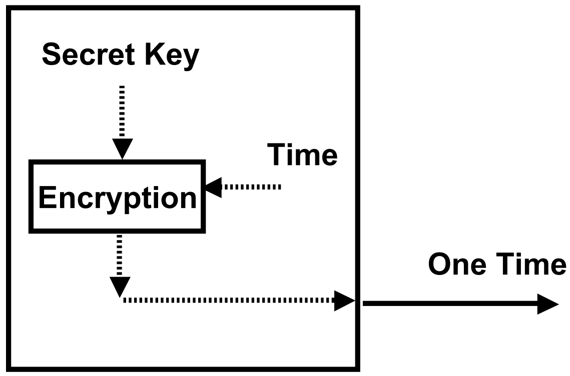
- Authentication
  - The first time, the user supplies $F^{(n-1)}(x)$.
  - The system checks if $F(F^{(n-1)}(x))=F^n(x)$. If yes, the user is authenticated and the system replaces $F^n(x)$ with $F^{(n-1)}(x)$.
  - The second time, the user supplies $F^{(n-2)}(x)$.
  - The third time, …



Time Synchronized

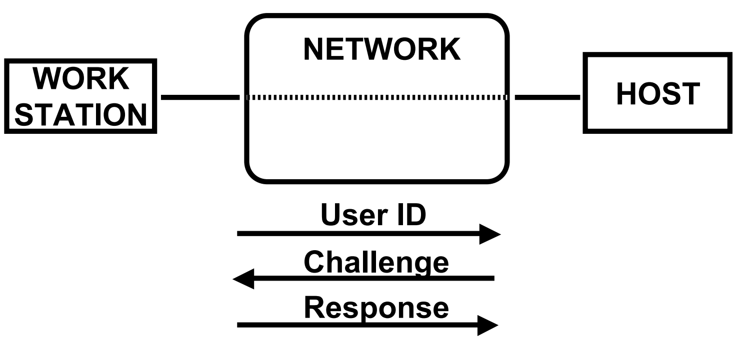
- There is a hand-held authenticator
  - It contains an internal clock, a secret key, and a display
  - Display outputs a function of the current time and the key
  - It changes about once per minute
- User supplies the user id and the display value
- Host uses the secret key, the function, and its clock to calculate the expected output
- The login is valid if the values match
- In practice, the clock skew is a problem

Time Synchronized (Cont'd)

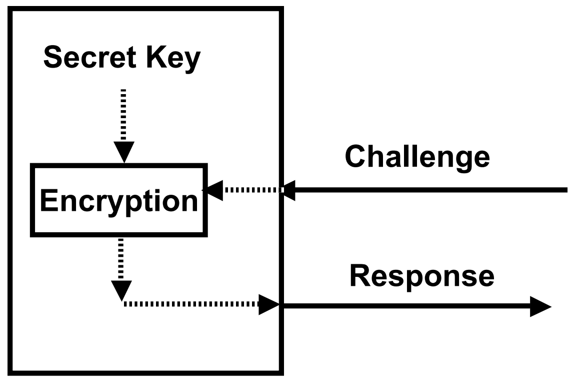


Challenge Response

- A non-repeating challenge from the host instead of a clock is used
- Note that the device requires a keypad.



Challenge Response (Cont'd)



Challenge Response (Cont'd)

- Problems with challenge/response schemes
  - Key database is extremely sensitive
  - This can be avoided if public key algorithms are used; however, the outputs would be too long for users to input conveniently

Biometrics

- Fingerprint
- Retina scan
- Voice pattern
- Signature
- Typing style

Biometrics (Cont'd)

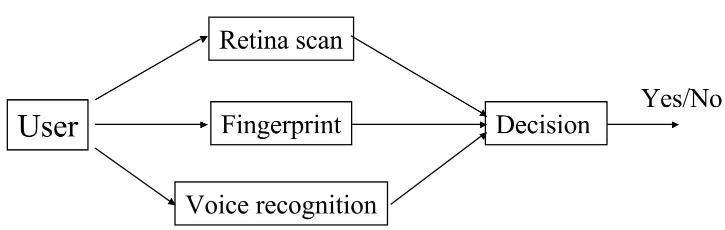
Technique	Description	Min. Cost	False Reading
Retina	Eyes scanned 1 to 2 inches from screening device	$2,400	1/10,000,000+
Iris	Camera image of eye takes from 14 inches	$3,500	1/131,000
Hand	Hand scanned on plate by three video cameras at different angles	$2,150	1/500
Fingerprint	Finger scanned on glass plate	$1,995	1/500
Signature	Written with special pen on digitizer tablet	$1,000	1/50
Voice	Predefined phrase spoken into telephone or microphone	$1,500	1/50

Effectiveness of Biometrics

- Two types of errors for authentication
  - False acceptance (FA)
    - Let imposters in
    - FAR: the probability that an imposter is authenticated.
  - False rejection (FR)
    - Keep authorized users out
    - FRR: the probability that an authorized user is rejected.
- Another type of error for identification
  - False match (FM)
    - One user is mistaken for another (legitimate user)
    - FMR: the probability that a user is incorrectly matched to a different user's profile.
- No technique is perfect!

Multimodal Biometrics

- Use multiple Biometrics together.
  - AND: Accept only when all are passed
    - Why do we need this?
  - OR: Accept as long as at least one is passed
    - Why do we need this?
  - Others



Summary

- Password authentication
  - Storing passwords
  - Dictionary attacks
  - Password Salt
- One-time passwords
  - S/Key
  - Time synchronized
  - Challenge response
- Biometrics