Authentication and Identification

Who? What? Where?

Overview of Today's Lecture:

- Username and Password
- Managing Passwords
- Choosing Passwords
- Spoofing Attacks
- Protecting the Password File
- Single Sign-On
- Alternative Approaches
- Summary

Username and Password:

- *Identification* – Who you are
- *Authentication* – You are who you claim to be

Entity Authentication

"The process of verifying a claimed identity"

- *TOCTTOU* – time of check to time of use

continued…

Repeated authentication

– *at start as well as during a session*

First line of defence

+ Widely accepted

+ Not too difficult to implement

- Managing passwords – *expensive*

- Common way of getting in

continued…

- forgotten passwords
- password guessing
- password spoofing
- compromise of the password file

Remember

User has a vital role in password protection

Managing Passwords:

- Password = a secret between user and system

Issues

- Password ends up in right hands?
- Interception?
- No password yet?

- New passwords – *delay ok*
- Forgotten passwords – *instant remedy necessary*

Choosing Passwords:

- Critical security issue
- Keeping probability of guessing to minimum

Guessing strategies:

- Exhaustive search – brute force
- Intelligent search – e.g. dictionary attack

continued…

Defences:

- Change default passwords
- Password length
- Password format
- Avoid obvious passwords

continued…

Further security improvements:

- Password checkers
- Password generation
- Password aging
- Limit login attempts

A combination of all those = highest security?

continued…

continued…

- People forget
- Contact an operator
- Opens a way for a new attack – *Social Engineering*

- Regularly used passwords best remembered

Tip - *don't change passwords before the weekend or holidays*

to remember…

- *Don't* look at security mechanisms in *isolation*
- Too much emphasis can *weaken* the system
- Users will try to *circumvent* security
- *Trade-off* between Complexity and Memory

Spoofing attacks:

- *Unilateral authentication* – one way
- No guarantee about end system

Spoofing attack

- e.g. Fake login screen

Prevention

- display failed login attempts
- trusted path (e.g. ctrl+alt+del)
- mutual authentication

continued…

Password caching

- password temporarily stored (buffer, cache, web page)
- beyond control of user
- sometimes for too long

This is another instance of *object reuse*.

Protecting the Password File:

- Password compared to an entry in a *password file*
- An attractive target for an attacker

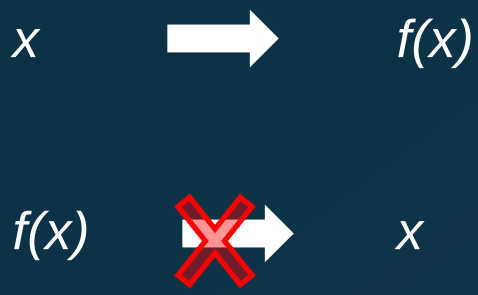
Protection

- Cryptography
- Access control enforced by the OS
- Combination of the above + attack delay

Cryptography:

One-way Function

A function that is relatively easy to compute but significantly harder to undo or reverse.



- *f(x)* is stored in the password file
- *f(x)* compared to computed f(x') from *x'* supplied by user

Access Control:

Access Control

Restricts access to files and resource to users with appropriate privileges

- Password file can’t be world readable
  - Off-line dictionary attacks
- or writeable
  - Change password

continued…

Password salting

Password + Additional Info (*Salt)* - > Encrypt

Remember

- Combination of mechanisms can enhance protection
- Separate security relevant and openly available data

(e.g. /etc/passwd and shadow password files)

Single Sign-On:

- Not convenient to repeatedly authenticate
- Whether one or multiple passwords

Single Sign-On

Password entered once. Stored by system and subsequently authenticating on your behalf.

- Convenient
- But new problems arise – storage of password

Alternative Approaches:

- Something you know
- Something you hold
- Who you are
- What you do
- Where you are

Something You Know:

- Knowledge of a “secret”
  - Password
  - PIN
  - Personal Details

- Anybody who obtains your secret = YOU
- No trace of passing secret to someone else
- Can you prove your innocence?

Something You Hold:

- Physical token
  - A key to a lock
  - Card (Smart cards, RFID cards)
  - Identity Tag

- Can be lost or stolen
- Again the one in possession becomes you
- Used in combination with something you know

Something You Are:

- Biometric schemes – unique physical characteristics
  - Face
  - Fingerprints
  - Iris patterns, etc…

- Accuracy of training and authentication
- “forged” fingers
- Mutilations
- Acceptable by users?

Biometrics:

1. *Enrolment* - Collection and storage of *reference templates*
2. *Identification* – Finding a user in a database of templates
3. *Verification* - Comparison against the reference template of identified user

Matching algorithm – calculates similarity between reference template and current reading. If similarity above certain threshold, accept user.

Biometrics:

False positives – Accepting the wrong user

False negatives – Rejecting a legitimate user

A balance needs to be found!

State-of-the-art fingerprint recognition schemes have error rates of around 1-2%

What You Do:

- Mechanical Tasks – repeatable and specific to individual
  - Handwritten signatures
  - Writing speed and pressure
  - Keyboard typing speed and intervals between keys

- Again needs to take into account *false positives* and *negatives*

Where You Are:

- Location of access
  - Operator console vs. arbitrary terminal
  - Office workstation vs. home PC
  - Geographical location

- IP address or GPS for locating users
- Not reliable on its own
- Should be used in combination with other mechanisms

To remember:

- A Password does not authenticate a person!

- Successful authentication = user knows a particular secret

- No way of distinguishing legitimate user and attacker who obtained the user's credentials

Summary:

- Passwords (creation, management)
- Attacks on passwords
- Alternative approaches

Next Week

Access Control

End