Authentication and Access Control

CS-576 Systems Security
Instructor: Georgios Portokalidis
Fall 2018
Overview

Authentication vs Authorization

Different means of authentication
  - Attacks and good practices

Different types of authorization
Authentication is the process of verifying an identity claimed by or for a system entity.

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.
Means/Factors of Authentication

- Something the individual knows
- Something the individual possesses
- Something the individual is/does
Something the User Knows

Password
- As56kf#dfjd8%d
- John123
- JustinBieber14
- Y3llow5ubm4rine

PIN
- 123456
- 654321
- 1248
- 338

Answers (to questions)
- What is the name of your dog?
- What is your favorite color?
- What... is the air-speed velocity of an unladen swallow?
Participants forgot 20% of their own answers within six months.

Acquaintance with whom participants reported being unwilling to share their webmail passwords were able to guess 17% of their answers.

... 13% of answers could be guessed within five attempts by guessing the most popular answers of other participants ...

It's no secret: Measuring the security and reliability of authentication via 'secret' questions

United Mileage Plus

Yesterday, Yan Zhu (@bcrypt) pointed out on Twitter that United Airlines Mileage Plus program has started collecting answers to security questions. They have a new twist: you must select one of a menu of answers.

United wants the answers to five questions, chosen from a list:

What is your favorite type of vacation?
What is your favorite sport?
What is your favorite flavor of ice cream?
During what month did you first meet your spouse or significant other?
What was the make of your first car?
Something the User Possesses
Something the Individual...

..Is

..does
Something the Individual...

..Is does

NOT just face recognition
Something the Individual...

..Is

..does
Something the Individual...

Is

How about CAPTCHA?

"Completely Automated Public Turing test to tell Computers and Humans Apart"
Multi-factor Authentication (MFA)

Require more than one methods/factors of authentication to be used
  - Not of the same type! For example, two passwords.

Most common instantiation: two-factor authentication (2FA)
Passwords

Widely used

Process

- User provides name/login and password
- System compares password with the one stored for that specified login

The user ID:

- Determines that the user is authorized to access the system
- Determines the user’s privileges
- Is used in discretionary access control
Password Transmission

HTTP

username: bob
password: p4ssw0rd
Password Transmission

username: bob
password: p4ssw0rd

Passive attacker
Password Transmission

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd
Password Transmission

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd

Passive attacker

Fall 2018
Stevens Institute of Technology
Password Transmission

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd

End-to-end security necessary

Fall 2018
Stevens Institute of Technology
19
Password Storage

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd

Raw
username: bob
password: p4ssw0rd
Password Storage

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd

Password DB leak

username: bob
password: p4ssw0rd
Password Storage

HTTP
HTTPS (TLS)

username: bob
password: p4ssw0rd

Password DB leak

Raw
username: bob
password: p4ssw0rd
## Password Leaks Happen All the Time

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Number of Leaked Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>RockYou Gaming</td>
<td>32.0 million</td>
</tr>
<tr>
<td>2010</td>
<td>Gawker Media</td>
<td>1.5 million</td>
</tr>
<tr>
<td></td>
<td>Domino attack</td>
<td>prompted resets in other</td>
</tr>
<tr>
<td></td>
<td>sites</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Sony</td>
<td>1.0 million</td>
</tr>
<tr>
<td>2012</td>
<td>LinkedIn</td>
<td>6.5 million</td>
</tr>
<tr>
<td>2013</td>
<td>Twitter</td>
<td>250,000</td>
</tr>
<tr>
<td></td>
<td>Before being</td>
<td>detected and shut down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Adobe</td>
<td>150.0 million</td>
</tr>
<tr>
<td>2015</td>
<td>ashley madison</td>
<td>15.26 million</td>
</tr>
</tbody>
</table>
Hashed Passwords

Password database stores a hashed version of the password
There are two approaches to attacking a secure hash function:

- **Cryptanalysis:** Exploit logical weaknesses in the algorithm
- **Brute-force attack:** Strength of hash function depends solely on the length of the hash code produced by the algorithm

MD5 and SHA-1 have been broken through cryptanalysis. SHA-2 or later is suggested.
Password Cracking

Dictionary attacks

Brute-force

Combination of the above

John the Ripper – first open-source password cracker developed in 1996
Dictionary Attacks

Develop a large dictionary of possible passwords and try each against the password file.

Each password must be hashed and then compared to stored hash values.

Good dictionaries and heuristics for combining words give attackers an advantage.

Publicly available databases of cracked passwords also help.
Dictionary Attacks

Develop a large dictionary of possible passwords and try each against the password file.

Each password must be hashed and then compared to stored hash values.

Rainbow Table Attacks

• Pre-compute tables of hash values
• Greatly accelerate attacking hashes
Adding Salt

A unique (possibly random) value (the salt) is added to the password before hashing.

![Diagram showing the process of adding salt to a password and the resulting hash code in a password file.](image-url)
Adding Salt

A unique (possibly random) value (the salt) is added to the password before hashing

Salts

- Make prevent the use of rainbow tables
- Make password attacks more expensive
- Hide whether multiple users use the same password
Efficiency of Password Attacks

Using DB of leaked password files, including the RockYou file.
An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Save Money. Save Time.

Whether it’s a WPA2 network, NTLM hashes, Unix hashes, or an encrypted PDF file, one thing’s for certain. By specializing in optimized cracking solutions and fine-tuning dictionaries from iteration to iteration, we can provide a solution that’s more effective, faster, and cheaper than anything else.

Comprehensive Dictionaries.

We have a range of dictionaries, fine-tuned for the format at hand. By extrapolating from our successes and iterating over our failures, we’ve been able to converge on the most effective wordlists for the money, every time.

Feel Safe Knowing We Found It.
Feel Secure If We Don’t.

Our jobs cost the same whether we find your password or not.

Simple To Use.

Submit your job in three quick steps, each one faster than the last.
http://hashcat.net/oclhashcat/
**Bcrypt()**

**bcrypt** is a password hashing function designed by Niels Provos and David Mazières, based on the Blowfish cipher.

**bcrypt** is an adaptive function:

- over time, the iteration count can be increased to make it slower
- It can remain resistant to brute-force search attacks
Password Reuse

Users tend to reuse the same password with multiple accounts

→ Exposure of one password leads to compromise of multiple passwords

→ Strong measures adopted by security-aware services can be invalidated by careless services
Phishing

Connect with your friends faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

Discover Facebook Mobile

Sign up

It's free (and will remain).

Name:
Surname:
Your email:
Re-enter your email address:
Password:
Gender:
Date of Birth:

Why do I have to provide my birthday?

Sign up
Phishing

Fake Browser with URL using HTML 5
A password manager offers an encrypted “wallet” for storing username/password pairs

Protected by password-based encryption

- A master password is used to derive a key for decrypting (unsealing) the wallet

Can defeat phishing, password reuse, poor password choices by

- Automatically filling in password based on domain
- Automatically generating strong passwords
- Eliminating the need to remember many passwords
Password Managers

Weaknesses:

- Compromise of the master password/wallet can be catastrophic
- Software may suffer from vulnerabilities
Alternatives -- Graphical Passwords
Alternatives -- Social Authentication

Instead of showing you a traditional captcha on Facebook, one of the ways we may help verify your identity is through social authentication. We will show you a few pictures of your friends and ask you to name the person in those photos. Hackers halfway across the world might know your password, but they don’t know who your friends are.
Token-based Authentication

Two major types

- Memory based (dumb) tokens
- Smart tokens
Memory Cards

Can store but do not process data
The most common is the magnetic stripe card
Can include an internal electronic memory
Can be used alone for physical access
  - Hotel room
  - ATM

Provides significantly greater security when combined with a password or PIN

Drawbacks of memory cards include:
  - Requires a special reader
  - Can be stolen
  - User needs to carry them
Smart Tokens

Physical characteristics:
- Include an embedded microprocessor
- A smart token that looks like a bank card
- Can look like calculators, keys, small portable objects

Interface:
- Manual interfaces include a keypad and display for interaction
- Electronic interfaces communicate with a compatible reader/writer

Authentication protocol:
- Two main categories:
  - Dynamic password generator
  - Challenge-response
Dynamic Protocol

Time-based One Time Password Generation

Valid for a limited amount of time

SECRET

OTP

SECRET
Simple Mutual Authentication (Challenge-Response)

**secret = H(password)**

- **Server sends sc**
- **Client sends cr + cc**
- **Server sends sr**
- **Generate unique random value sc (nonce)**
- **Generate cr and check received value**
- **Generate sr and check received value**

Generate unique random value **cc** and calculate
**cr = H(cc + sc + secret)**

Generate **sr** and check received value
Challenge-Response Protocol

Using public-key cryptography

Secret key PK⁺

Public key PK⁻

Verify signature

Generate unique random value cc

Server sends \( \text{sc+SIG(PK}⁻, \text{sc)} \)

Generate unique random value sc (nonce)

Client sends \( \text{cr+SIG(PK}⁺, \text{cr)} \)

Verify signature
Security Issues with Cards

Information may be unencrypted on the card

They can be reverse engineered
Biometric Authentication

Attempts to authenticate an individual based on unique physical characteristics

Based on pattern recognition

Is technically complex and expensive when compared to passwords and tokens

Physical characteristics used include:

- Facial characteristics
- Fingerprints
- Hand geometry
- Retinal pattern
- Iris
- Signature
- Voice
Cost vs Accuracy for Biometrics

- Hand
- Signature
- Face
- Voice
- Iris
- Retina
- Finger

Cost vs Accuracy Graph
Figure 3.8  A Generic Biometric System. Enrollment creates an association between a user and the user’s biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.
Probability density function

![Diagram](image)

- **Imposter profile**
- **Profile of genuine user**
- **False nonmatch possible**
- **Decision threshold \( t \)**
- **False match possible**
- **Average matching value of imposter**
- **Average matching value of genuine user**

**Figure 3.9 Profiles of a Biometric Characteristic of an Imposter and an Authorized User**

In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value \( s \) is greater than a preassigned threshold \( t \), a match is declared.
Operating Characteristic Curves

- Idealized measurement
- log-log scale

Equal-error rate (ERR) is an important metric. Lower is better.
Figure 3.11  Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.
Access Control

Reference monitor

User -> Access request

Policy

Resources
Access Control Approaches

Discretionary Access Control (DAC)
- Resources are usually associated with an owner
- Discretionary because the owner can delegate access

Mandatory Access Control (MAC)
- Operating system or reference monitor strictly manages access
- Access can not be delegated
DAC Example: UNIX Permissions

Entities
- User owner
- Group
- Others

Resource
File Object

Access type
- RWX
- RWX
- RWX
### MAC Example: Access control list (ACL)

<table>
<thead>
<tr>
<th>Entity</th>
<th>Access type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 
- 
- 
- 

Resource

File Object
Role-based Access Control (RBAC)

Policies apply on roles

- Roles are similar to groups

Usually less roles than users → easier management

Easy to handle users switching roles

DAC or MAC afterwards
Role Hierarchy

More rights

Administrator

PowerUser

User

Less rights

Guest
Mix and Match

In practice multiple approaches are usually combined to control different type of requests and resources