User Authentication

Prof. Federica Paci

Lecture Outline

- Password Based Authentication
  - Password Attacks
  - Possible Countermeasures
- Stronger Authentication Techniques → ci sono molti metodi di autenticazione che vanno oltre alla password
  - Multi-factor Authentication (MFA)
    - OTP authentication
    - Biometric Authentication

Authentication

- The determination of **identity**, usually based on a combination of
  - something the person knows (like a password),
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person is (like a human with a fingerprint)

Something you are

Something you know

Something you have

Gates predicts death of the password

predetto 20 anni fa → le password sono la causa dell'80% delle violazioni di sicurezza

↓ rimane comunque ora il metodo predefinito per molti servizi

↳ infatti è:
- economico
- facile da implementare
- comprensibile per gli utenti

Traditional password-based security is headed for extinction, says Microsoft's chairman, because it cannot "meet the challenge" of keeping critical information secure.

Munir Kotadia

Feb. 25, 2004 1:27 p.m. PT

3 min read

SAN FRANCISCO--Microsoft Chairman Bill Gates predicted the demise of the traditional password because it cannot "meet the challenge" of keeping critical information secure.

Gates, speaking at the RSA Security conference here on Tuesday,

Password Authentication

- widely used user authentication method
  - user provides username and password
  - system compares password with that in the password file
- authenticates ID of user logging and
  - that the user is authorized to access system
  - audit logs

Password Authentication is not secure

Dani creati
1 Di reputazione
2 Economici

Password Overload

Tutto nasce dalla necessità di usare molto spesso le password per accedere ad alcuni servizi

porta gli utenti a NON sviluppare delle goodpractices

Predictable passwords

facilmente memorizzabili

ovvero facilmente attaccabili

Top 10 Worst Password of 2022

1. 123456
2. 12345
3. password
4. usr
5. 123456789
6. 1234
7. 12345678
8. qwerty
9. 147258369
10. 123

- Uso di schemi prevedibili di password per far fronte alle numerose password necessarie per i vari servizi
  - ↳ sfruttato dagli attaccanti

Password Reuse

- Riuso della stessa password per usri servizi → NO good practies
  ↳ sfruttato dagli attaccanti

  52% delle password viene riusato tra gli account

In the past year, 2 in 5 people:

Received a notice that their personal information had been compromised

Had an account hacked

Had a password stolen

63% of Data Breaches Result From Weak or Stolen Passwords

Una password non consona è la causa principale dei data breach

Tweet Share 28 Like 3 Share G+

In its recent **2016 Data Breach Investigations Report**, Verizon Enterprise confirmed many industry trends that we see at ID Agent every day. The most glaring blind spot for organizations is how stolen credentials are the primary means by which hackers exploit their vital systems.

Credentials are the holy grail for hackers. In a study of 905 phishing attacks, the vast majority—91 percent—were after user credentials.

Stolen Credentials Are a Big Problem That You May Not Know About

Type of Attacks

Offline Attacks

Active Online Attacks

Passive Online Attacks

Non Technical Attacks

How passwords are cracked

una password può essere rubata in moltissimi modi, alla fine permetterà comunque l'accesso fraudolento all'utente se il furto ha avuto successo

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Interception

Passwords can be intercepted as they are transmitted over a network.

Shoulder Surfing

Observing someone typing their password.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Searching

IT infrastructure can be searched for electronically stored password information.

Key Logging

An installed keylogger intercepts passwords as they are typed.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Where are the passwords stored?

- Windows
  - Local machines: SAM database
  - C:\Windows\System32\config
  - Mounted as a HKLM/SAM
- Linux
  - Local machines: etc/passwd and etc/shadow

How are the passwords stored?

gruppo a cui appartiene l'utente

User SID HASHES

```
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:214c1f5d621f7dbbbc7b0f552c530719:c1c40b8b19e995748bba99667e3049d6:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:af01dfe386ba890a36e779f03a8f0a42:::
Fred:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Fede:1004:bf6055b589337675e68aa26a841a86fa:ec8d06918467bb62e0ce0fb39444a33e:::
SUPPORT:1005:9c2a030f0b086b69aad3b435b51404ee:b23a90d0aad9da3615fafc27a1b8baeb:::
```

LM vs NTLM Hashes

Sono due algoritmi di hashing utilizzati per la memorizzazione delle password in sistemi operativi Microsoft Windows

LM

↳ Lan Manager

prima del 2000
tenuto per retrocompatibilità

considerato obsoleto ed insicuro

non più utilizzato

usa un algoritmo hash più debole

128 bits
Character set: 142
Max length: 14 characters
Password split in two 7 char strings
Case insensitive

supporta solo caratteri alfanumerici e alcuni simboli speciali

lo rende vulnerabile agli attacchi di forza bruta

NTLM

↳ New Technology Lan Manager

versione migliorata e più sicura di LM

è stato sostituito in molti contesti più recenti da protocolli più sicuri come Kerberos, NTLM è ancora utilizzato in alcune configurazioni di rete

usa algoritmo hash più robusto

128 bits
Character set: 65000
Max length: 256 characters
Based on the entire password
Case Sensitive

supporta anche caratteri speciali e caratteri unicode

utilizza un algoritmo più complesso

Windows' Password Hashes

- LM Hashes store passwords up to 14 characters
- All letters are converted to UPPER case
- Padded with blank characters to fill out all 14 characters
- Then split in two strings of 7 characters
- Each 7 character string is then encrypted and combined back

Password	BatmanRules
Converted to Upper Case	BATMANRULES
Padded	BATMANRULES---
Split	BATMANR ULES---

Windows' Password Hashes

- LM Hashes store passwords up to 14 characters
- All letters are converted to UPPER case
- Padded with blank characters to fill out all 14 characters
- Then split in two strings of 7 characters
- Each 7 character string is then encrypted and combined back

Encrypted

BATMANR
86D8D0AEB8D112F8

ULES---
F9954FC9DF7E012

uses DES che non è considerato sicuro

Combined

86D8D0AEB8D112F8
F9954FC9DF7E012

Brute Force Attacks

- Exhaustive search
  - Try all possible combinations of symbols up to a certain length
  - The size of the password space is $|A|^n$
- Assume a 8 characters password
  - Upper- and lowercase letters, digits, common symbols (96 possible characters)
  - 96^8 = 7.2 quadrillion password combinations

Dictionary Attack

- Attacker tries passwords from a “dictionary” of commonly used passwords and compares with encrypted or hashed password
- The dictionary is a text file that can be downloaded
  - Languages
  - Characters
  - Famous people, locations, regions
- This attacks with current processor speeds take hours or days or even less

Hybrid Attack

- Using a dictionary
- Trying different variations including special characters and numbers

Rainbow Tables

- Precomputed compilation of plaintext passwords and matching hashes
- They are faster in cracking passwords than brute-force, dictionary attacks and hybrid attacks
- They occupy a lot of memory

Sfrutta la precalcolazione di hash crittografici. Le tabelle contengono coppie di valori chiari (come password) e corrispondenti hash, ma in forma ottimizzata per accelerare il processo di ricerca
Metodo efficace contro password deboli o comuni.
Per mitigare questi attacchi è necessario usare algoritmi di hash robusti, viene anche aggiunto un valore casuale per rendere l'hash unico anche per la stessa password sconfiggendo l'efficacia delle rainbow tabels precalcolate

il salt

Pass-the-Hash

How long does it take to crack a password?

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

Password strength

- Password **strength** measures the effectiveness of a password against **brute brute-force** attacks
- It is normally computed as log2 ($|A|^n$)
  - A is the set of symbols composing the password
  - N is the length of the password
- For example
  - If the password contains only lowercase letters |A| = 26
  - The length of the password is 8
  - The entropy will be log 2 (26^8) = 37.60
  - The password is weak
- A strong password has an entropy of at least 60 bits

Which password is more secure?

- Go to https://users.ece.cmu.edu/~lbauer/pwdquiz/
- sponge01bob or spongebob01?
- pAssewOrd or p@ssw0rd?
- Thefirstkiss or 1qaz2wsx3edc?

Password strength

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

zxcvbn

tiene conto dei pattern

	qwER43@!	Tr0ub4dour&3	correcthorsebatterystaple
zxcvbn	Weak	So-so	Great!
Dropbox (old)	Great!	Great!	So-so
Citibank	Medium	Strong	1 number required

zxcvbn

- Assume a password as consisting of one more concatenated patterns
- The patterns are :

Pattern	Example
Token	Logitech, parlamentarian
Reversed	DrowssaP
Sequence	123 2488 jklm
Repeat	zzz ababab
Keyboard	qwertyuio
Date	7/8/1947 8.7.47 11.7.21
Bruteforce	X$JQhMzt

zxcvbn

- Match → Estimate → Search
- Input: lenovo1111

lenovo	token
eno	backwards
no	english
no	backwards (on)
1111	date
1111	repeat

zxcvbn

- Match → **Estimate** → Search
- Input: lenovo1111

lenovo	token	11007 guesses
eno	backwards	3284 guesses
no	english	11 guesses
no	backwards	18 guesses
1111	date	2190 guesses
1111	repeat	48 guesses

zxcvbn

- Match → Estimate → Search
- Input: lenovo1111

lenovo	token	11007 guesses
~~eno~~	~~backwards~~	~~3284 guesses~~
~~no~~	~~english~~	~~11 guesses~~
~~no~~	~~backwards~~	~~18 guesses~~
~~1111~~	~~date~~	~~2190 guesses~~
1111	repeat	48 guesses

Countermeasures

- Password salting
  - Append to the password a random number (salt)
  - If the salt is *b* bits, the number of possible passwords is increased of factor 2^b
- Password file access control
  - Restrict access only to privileged users
  - Keep the hashed passwords separated from userIDs
- Fast reissuance of password

Online Dictionary Attack

i criminali per accedere possono provare le password più ovvie che milioni di persone continuano ad utilizzare

- Intelligent search
  - Try passwords associated with the user
    - e.g name, name of friends, car brand
  - Try words in a dictionary
  - Try popular passwords
- Save attacker's time
- No guarantee the right password is found

Credential Stuffing

Il modo più comune in cui le password possono essere rubate sono i data breach.
I criminali utilizzeranno le password rubate per cercare di accedere ad altri account.

Password spraying

Possible Countermeasures

- Password policies
  - Set password length: minimal password length should be prescribed
  - Set Password format: mix upper and lower case, symbols, numerical, and non-alphabetical symbols
  - Avoid obvious passwords:123456, John3:16, Monster1, Chicken1, …
- Changing passwords
  - Force users to change passwords regularly
- Machine-generated passwords
  - Pronounceable passwords are generated for the user

A prescindere da come le password vengono acquisite, a meno che non venga implementato un metodo aggiuntivo di autenticazione, i criminali possono utilizzare le credenziali rubate per accedere in modo fraudolento agli account degli utenti.

Effective countermeasures

The logic behind three random words

Whilst not a password panacea, using 'three random words' is still better than enforcing arbitrary complexity requirements.

Effective countermeasures

- Lockout mechanics
  - Lock user account after several unsuccessful login attempts
- Throttling
  - Time delays are introduced between consecutive failed login attempts
- Security monitoring
  - Monitoring login to detect unusual use
  - Notify the user with details of attempted login
- Password blacklisting
  - Check if an input password is in a list of common words

Interception

- Clear text password is intercepted by the attacker
- **Countermeasure:** Encrypt the communication among users and web site e.g SSL/TLS protocols

Keylogger

- Small program that monitors each keystroke the user types on his keyboard
- Installed by attaching the program to an image or file and then send it via email
- Popular keyloggers
  - Refog
  - Revealer
  - KidLogger

Social Engineering

- Phishing
  - Sending an email asking to reset the password
- Shoulder-surfing
  - Attacker gathers passwords by watching over a person's shoulder while he/she is logging in

attacchi IRL

- Dumpster-diving
  - Attacker look into the trash for piece of papers or documents with written passwords
- Countermeasure: User Awareness and Training

Summary

- Password based authentication systems are not secure
  - Users use ease to guess passwords
  - Users reuse passwords across multiple web sites
- Password based authentication systems are vulnerable to various attacks
  - Social engineering and data breaches are on top of the list
- Effective countermeasures are
  - Account lockout and throttling
  - Predictive monitoring
  - Password blacklisting

Resources

- NCSC. Password Guidance: Symplifying your approach. Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
- NIST. New Digital Identity Guidelines. Available at: https://pages.nist.gov/800-63-3/
- zxcvbn: Low-Budget Password Strength Estimation. Available at: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

Multi – factor authentication

- Accounts that have been set up with MFA require the user to provide a second factor, which is something that only the user can access

- The second factor can include:
  - PIN codes or a string of characters, often sent to the user via SMS or email
  - a security token that the user must physically connect to their device (such as via USB)
  - biometric details (such as a fingerprint scan, or facial recognition)
  - an app on a trusted device (such as those provided by Microsoft or Google)

One-Time Passwords

Two widely used methods to get that one time password:

- **SMS-based**: In this method, every time the user logs in, they receive a text message to their registered phone number, which contains a One Time Password

- **TOTP-based**: In this method, while enabling 2-factor authentication, the user is asked to scan a QR image using a specific smartphone application. That application then continuously generates the One Time Password for the user.

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

The HOTP client (hardware or software token) increments its counter and then calculates the next HOTP value HOTP client. If the value received by the authentication server matches the value calculated by the client, then the HOTP value is validated. In this case, the server increments the counter value by one.

HMAC-Based One Time Password Algorithm(HOTP)

1. The user enables two factor authentication
2. Backend server creates a secret key for that particular user

2. Server then shares that secret key K with the user's phone application.

3. Phone application initializes a counter C

4. Phone application first increments the counter value by one and then generates a one-time password using that secret key and counter as follows:

$$HOTP(K, C) = Truncate(HMAC\text{-}SHA1(K,C))$$

6. If the value sent by the phone application matches the one generated by the server, the server increments the counter value by one

The prover (e.g., token, soft token) and verifier (authentication or validation server) MUST know or be able to derive the current Unix time (i.e., the number of seconds elapsed since midnight UTC of January 1, 1970) for OTP generation.

Time-based One Time Password

- The only difference is that it uses “Time” in the place of “counter”
- The phone application and the server do not need to initialize the counter and keeping track of it
- As a server and phone both have access to time, neither of them has to keep track of the counter
- The phone application and the server MUST know or be able to derive the currentUnix time (i.e., the number of seconds elapsed since midnight UTC of January 1, 1970) for OTP generation

$$TOTP(K, C) = HMAC\text{-}SHA256(K,T) \text{ where}$$

$$T = (\text{Current Unix time} - T_0)/X$$

X represents the time steps in seconds

T_0 is the Unix time to start counting time steps

Biometrics

- **Biometric** refers to any measure used to uniquely identify a person based on biological or physiological traits.
- Generally, biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before granting access.

Image from http://commons.wikimedia.org/wiki/File:Fingerprint_scanner_in_Tel_Aviv.jpg used with permission under the Creative Commons Attribution 3.0 Unported license

Biometrics in real life

Requirements for Biometric Autthentication

- **Universality.** Almost every person should have this characteristic.
- **Distinctiveness.** Each person should have noticeable differences in the characteristic.
- **Permanence.** The characteristic should not change significantly over time.
- **Collectability.** The characteristic should have the ability to be effectively determined and quantified.

Candidates for Biometric IDs

- Signature
- Fingerprints
- Retinal/iris scans
- DNA
- Voice recognition
- Face recognition
- Gait recognition

Public domain image from
http://commons.wikimedia.org/wiki/File:Fingerprint_Arch.jpg

Public domain image from
http://commons.wikimedia.org/wiki/File:Retinal_scan_securimetrics.jpg

Public domain image from
http://commons.wikimedia.org/wiki/File:CBP_chemist_reads_a_DNA_profile.jpg

New candidates for biometric IDs

Boffins take biometric logins to heart, literally: Cardiac radar IDs users to unlock their PCs

2026, when a change of heart will mean a pretty bad day

By Katyanna Quach 26 Sep 2017 at 05:01 20 SHARE ▼

Image credit: Bob Wilder/University at Buffalo

Biometric Identification

Biometric Authentication

- Limitations
  - Accuracy of matching algorithm
    - False positives: allow access to unauthorized user
    - False negatives: reject a legitimate user
  - Easy forging of biometric traits
    - Fingerprints left in many places
  - Low user acceptance
    - User may not like to have their retina scanned

An HMAC-Based One-Time Password Algorithm

Resources

- HOTP – An HMAC-based One Time Password Algorithm. https://www.rfc-editor.org/rfc/rfc4226
- TOTP- Time-based One Time Password.Algorithm. https://www.rfc-editor.org/rfc/rfc6238
- Authentication methods: choosing the right type. https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type