

Session 02  
Authentication

Security of Information Systems (SIS)

Computer Science and Engineering Department

October 11, 2023

Notes

---

---

---

---

---

---

---

---

1 / 40

Access Control Terms

- ▶ authentication
- ▶ authorization
- ▶ access control

Notes

---

---

---

---

---

---

---

---

2 / 40

Papers

- ▶ On the Accuracy of Password Strength Meters (ACM CCS 2018)
- ▶ Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition (ACM CCS 2016)

Notes

---

---

---

---

---

---

---

---

3 / 40

Model

- ▶ actor / subject / agent
- ▶ credentials database (role, permissions, access control list)
- ▶ resource / object
- ▶ reference monitor

Notes

---

---

---

---

---

---

---

---

5 / 40

## Credentials

- ▶ who you are
- ▶ what you have
- ▶ what you know

6 / 40

Notes

---

---

---

---

---

---

---

---

## Credential Types

- ▶ biometric
- ▶ hardware tokens
- ▶ software tokens
- ▶ secret (password)

7 / 40

Notes

---

---

---

---

---

---

---

---

## Biometrics

- ▶ fingerprint
- ▶ face
- ▶ iris
- ▶ voice
- ▶ keystroke dynamics

9 / 40

Notes

---

---

---

---

---

---

---

---

## Hardware Tokens

- ▶ access card
- ▶ hardware keys
- ▶ one-time password (OTP)

10 / 40

Notes

---

---

---

---

---

---

---

---

- ▶ certificate
- ▶ kerberos ticket
- ▶ cookie

---

---

---

---

---

---

---

---

---

---

Passwords

- ▶ string of printable characters (ASCII)
- ▶ protect access
- ▶ stored in a password database and requested at each login/authentication
- ▶ most common method of authentication

---

---

---

---

---

---

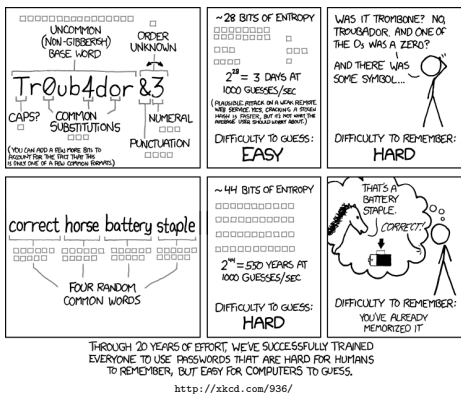
---

---

---

---

Password Cracking Context (1)




---

---

---

---

---

---

---

---

---

---

Password Cracking Context (2)

Character set	Password length					
	5	6	7	8	9	10
0-9	1.00e05	1.00e06	1.00e07	1.00e08	1.00e09	1.00e10
a-z	1.19e07	3.09e08	8.03e09	2.09e11	5.43e12	1.41e14
a-z,0-9	6.05e07	2.18e09	7.84e10	2.82e12	1.02e14	3.66e15
a-z,0-9,3 punct	9.02e07	3.52e09	1.37e11	5.35e12	2.09e14	8.14e15
a-z,A-Z	3.80e08	1.98e10	1.03e12	5.35e13	2.78e15	1.45e17
a-z,A-Z,0-9	9.18e08	5.68e10	3.52e12	2.18e14	1.35e16	8.39e17
a-z,A-Z,0-9,32 punct	7.34e09	6.90e11	6.48e13	6.10e15	5.73e17	5.39e19

<http://hitachi-id.com/password-manager/docs/password-management-best-practices.pdf>

---

---

---

---

---

---

---

---

---

---

## Passwords vs. Passphrases

- ▶ a password is a word and a passphrase is a set of words
- ▶ passphrases usually has spaces
- ▶ passphrases are recommended due to their increased length and being easier to remember

16 / 40

Notes

---

---

---

---

---

---

---

---

## Attacker

- ▶ online attack
  - ▶ "live" attack
  - ▶ run client/application, feed passwords and try to match
- ▶ offline attack

17 / 40

Notes

---

---

---

---

---

---

---

---

## Scenario 1: Plaintext

- ▶ attacker
  - ▶ gain access to database
  - ▶ profit!
- ▶ defender
  - ▶ database access control
  - ▶ one-way function

18 / 40

Notes

---

---

---

---

---

---

---

---

## Cryptographic Hash Functions

- ▶ deterministic
- ▶ uniformity
- ▶ infeasible to reverse
- ▶ highly dynamic
- ▶ usually very fast

20 / 40

Notes

---

---

---

---

---

---

---

---

## Hash Security Properties

- ▶ pre-image resistance
- ▶ second pre-image resistance
- ▶ collision resistance

21 / 40

Notes

---

---

---

---

---

---

---

---

## Hash Algorithms

- ▶ SHA1
- ▶ MD2, MD4, MD5
- ▶ SHA2
- ▶ bcrypt
- ▶ SHA3

22 / 40

Notes

---

---

---

---

---

---

---

---

## Scenario 2: Hashed Password

- ▶ attacker
  - ▶ rainbow tables
  - ▶ profit!
- ▶ defender
  - ▶ salt

23 / 40

Notes

---

---

---

---

---

---

---

---

## Rainbow Tables

- ▶ database of hashes
- ▶ space vs time

24 / 40

Notes

---

---

---

---

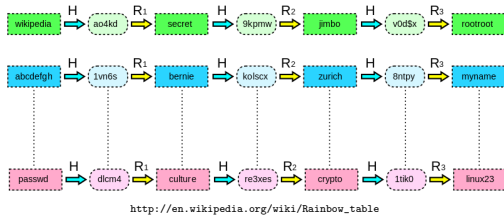
---

---

---

---

## Rainbow Tables (2)



25 / 40

Notes

---

---

---

---

---

---

---

---

---

---

## Salt

- ▶ additional input
- ▶ concatenated with the password
- ▶ one per password

26 / 40

Notes

---

---

---

---

---

---

---

---

---

---

## Scenario 3: Salted hashes

- ▶ attacker
  - ▶ dictionary / hybrid attack
  - ▶ brute-force attack
  - ▶ side-channel attacks
  - ▶ profit !?!
- ▶ defender
  - ▶ policies
  - ▶ defensive programming

27 / 40

Notes

---

---

---

---

---

---

---

---

---

---

## Dictionary Attacks

- ▶ use a dictionary/word list
- ▶ go through word list, compute hash and compare to password hash
- ▶ simple form of attack
- ▶ relies on people using simple passwords

28 / 40

Notes

---

---

---

---

---

---

---

---

---

---

- ▶ <http://wiki.skullsecurity.org/Passwords>
- ▶ <https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm>
- ▶ <http://security.stackexchange.com/questions/9567/modern-high-quality-password-dictionary>

29 / 40

Notes

---

---

---

---

---

---

---

---

## Hybrid Attack

- ▶ use a dictionary
- ▶ apply mutations for each word
  - ▶ combine dictionary words
  - ▶ change i to 1, s to 5, e to 3
  - ▶ change cases
  - ▶ add 123 at the end of the word
  - ▶ add ! at the end of the word
- ▶ hash and check with password hash

30 / 40

Notes

---

---

---

---

---

---

---

---

## Policy

- ▶ complexity
  - ▶ password length
  - ▶ charset
- ▶ password expiration
- ▶ password reuse

31 / 40

Notes

---

---

---

---

---

---

---

---

## Policy Issues

- ▶ password security paradox
  - ▶ easy to remember
  - ▶ hard to guess
- ▶ user behavior
- ▶ solution: password managers

32 / 40

Notes

---

---

---

---

---

---

---

---

## Side-Channel Attacks

- ▶ timing information
- ▶ performance / power consumption
- ▶ electromagnetic leak
- ▶ acoustic information
- ▶ social engineering
- ▶ rubber-hose technique

33 / 40

Notes

---

---

---

---

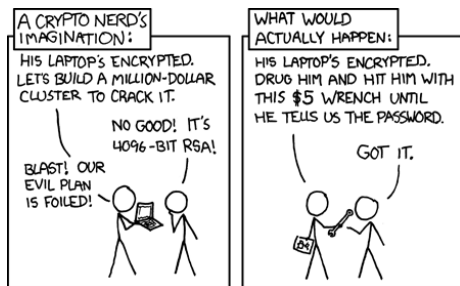
---

---

---

---

## Rubber-hose Technique



<http://xkcd.com/538/>

34 / 40

Notes

---

---

---

---

---

---

---

---

## Recommendations

- ▶ do not use unsafe hashing algorithms!!!
- ▶ passphrase > complex password
- ▶ use / allow password managers
- ▶ use 2FA / 3FA
- ▶ secure side channels

36 / 40

Notes

---

---

---

---

---

---

---

---

## Common tools

- ▶ John The Ripper
- ▶ RainbowCrack
- ▶ HashCat

37 / 40

Notes

---

---

---

---

---

---

---

---



## Keywords

- ▶ credentials
- ▶ password
- ▶ passphrase
- ▶ hash functions
- ▶ rainbow tables
- ▶ salt
- ▶ dictionary attack
- ▶ side-channel attack
- ▶ policies
- ▶ social engineering
- ▶ shoulder surfing
- ▶ one-time password
- ▶ password complexity
- ▶ password manager
- ▶ 2/3 factor authentication
- ▶ SHA256, SHA512
- ▶ sHA3
- ▶ rubber-hose technique

38 / 40

Notes

---

---

---

---

---

---

---

---

---

---

## Nice to read

- ▶ Targeted Online Password Guessing: An Underestimated Threat (ACM CCS 2016)
- ▶ On the Accuracy of Password Strength Meters (ACM CCS 2018)
- ▶ Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition (ACM CCS 2016)
- ▶ An Empirical Study of Mnemonic Sentence-based Password Generation Strategies (ACM CCS 2016)

39 / 40

Notes

---

---

---

---

---

---

---

---

---

---

## Nice to read (2)

- ▶ Password Cracking Techniques
- ▶ Breaking the iris scanner locking Samsung's Galaxy S8 is laughably easy
- ▶ Galaxy S8 face recognition already defeated with a simple picture
- ▶ Bypassing TouchID was "no challenge at all," hacker tells Ars
- ▶ Behavioral Profiling: The password you can't change.

40 / 40

Notes

---

---

---

---

---

---

---

---

---

---

Notes

---

---

---

---

---

---

---

---

---

---