Session 02

Authentication

Security of Information Systems (SIS)

Computer Science and Engineering Department

October 11, 2023

Access Control Terms

- authentication
- authorization
- access control

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)

Model

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

Credentials

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

Credential Types

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

Biometrics

- fingerprint
- face
- iris
- voice
- keystroke dynamics

Hardware Tokens

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

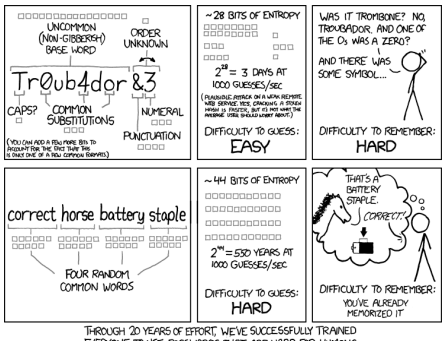
Software Tokens

- 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)



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.

http://xkcd.com/936/

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	9.16e08	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

Attacker

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

Scenario 1: Plaintext

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

Cryptographic Hash Functions

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

Hash Security Properties

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

Hash Algorithms

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

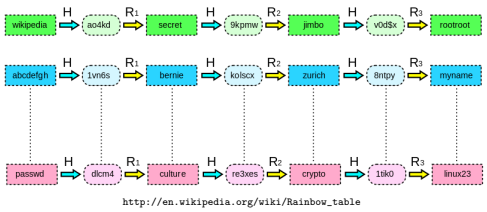
Scenario 2: Hashed Password

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

Rainbow Tables

- database of hashes
- space vs time

Rainbow Tables (2)



Salt

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

Scenario 3: Salted hashes

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

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

Password Dictionaries / Word Lists

- 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

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

Policy

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

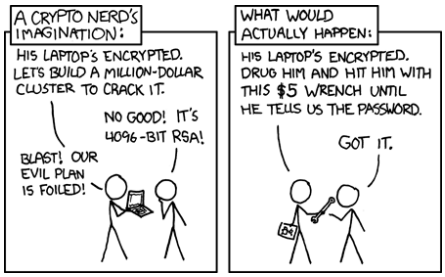
Policy Issues

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

Side-Channel Attacks

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

Rubber-hose Technique



http://xkcd.com/538/

Recommendations

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

Common tools

- John The Ripper
- RainbowCrack
- HashCat

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

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)

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.