



Oregon State
University

COLLEGE OF ENGINEERING | School of Electrical Engineering
and Computer Science



User Authentication

What is Authentication?



Oregon State University
College of Engineering

Verifying that something is genuine or someone is who they claim they are

- Example:
 - Photo ID check before boarding a plane
 - Authenticating an antique painting



In computer security – binding an external entity to a system entity

Authentication Basics



Oregon State University
College of Engineering

- Authentication: binding of subject to principal
 - subject represents an external entity (you, me, Amazon store, *etc.*)
 - principal is computer entity (process, network connection, *etc.*)
- Two steps
 - Identification step: present identifier to the security system.
 - Verification step: Present or generate authentication information that corroborates the binding between entity and identifier

Establishing Identity



Oregon State University
College of Engineering

- Authentication Factors
 - What entity knows (*e.g.* password, private key)
 - What entity has (*e.g.* badge, smart card)
 - What entity is (*e.g.* fingerprints, retinal characteristics)
 - What entity does (*e.g.*, voice pattern, handwriting, typing rhythm)
 - Where entity is (*e.g.* in front of a particular terminal)*
- Multi-factor authentication
 - Use multiple elements/factors to prove identity
 - Example: Chip and PIN credit card transaction or debit card transactions

Complementation Information



Oregon State University
College of Engineering

- User provides information to verify identity during registration
- System stores a processed version of this information as the *complementation* information
- The complementation function maps from the user provided data to the system stored data
 - Need to worry about access to user provided data

Password-based Authentication



Oregon State University
College of Engineering

- External entity is bound to system ID (user account)
- Authentication Step
 - External entity presents password
 - System compares with previously stored password
 - If password matches, system starts process with bound ID
- Later access control and privilege decisions made against ID

Authentication and Access Control



Oregon State University
College of Engineering

- Typically, authentication is a critical first step for access control
- Example:
 - Photo ID check before boarding a plane (authentication)
 - Boarding pass check before boarding a plane (authorization or access control)

Summary



Oregon State University
College of Engineering

- Authentication is establishing identity
 - binding an external identity to a system identity
- Multiple factors of authentication
 - what you know
 - what you have
 - what you are
 - what you do
- Authentication is critical first step in access control



Password Based Authentication: Pros and Cons I

Password-based Authentication



Oregon State University
College of Engineering

- External entity is bound to system ID (user account)
- Authentication Step
 - External entity presents password
 - System compares with previously stored password
 - If password matches, system starts process with bound ID
- Later access control and privilege decisions made against ID

Password Systems - Advantages



Oregon State University
College of Engineering

- Password-based authentication has been around since 60s
 - It is widely used
- Why?
 - easy to implement
 - no special software needed on clients or servers
 - less expensive
 - no special hardware needed at the client side
 - easier to replace/recover
 - password reset (compare with tokens or biometrics)

Password Systems – Issues/Vulnerabilities



Oregon State University
College of Engineering

- Password Selection/Strength
- Password Storage
- Password Sharing/Re-use
- Social-engineering/Pre-texting
- Trusted Path/Electronic Monitoring
- System Design

Password Selection



Oregon State University
College of Engineering

- Naïve passwords
 - People pick easy to remember passwords
 - easy to guess/break – weak passwords
 - Examples: 'iloveyou', 'password', '123456', 'asdfgh' etc.
- Lists of common passwords readily available
 - Millions of leaked passwords available to train “crackers”

Password Selection



Oregon State University
College of Engineering

- Random passwords
 - any password from possible set equally likely
 - hard to guess/break but hard to remember
- USERS' TASK: "choose a password you can't remember, and don't write it down"

Password Selection: Memorability vs. Strength



Oregon State University
College of Engineering

- Research Nuggets
 - System Generated Pronounceable Passwords
 - Longer passwords
 - Passphrases

System Generated Pronounceable Passwords



Oregon State University
College of Engineering

- Generate phonemes randomly
 - Phoneme is unit of sound
 - Examples: helgoret, juttelon are; przbqxdfi, zxrptglfn are not
- ~ 440 possible phonemes
- 440^6 possible keys with 6 phonemes (12-18 characters long), about the same as 96^8
- Used by GNU Mailman mailing list software

Longer Passwords



Oregon State University
College of Engineering

- Lorie Cranor's group (CMU) found that
 - 16 character passwords \geq shorter passwords (e.g. 8) with symbols, numbers, caps etc

Passphrases

- Use a phrase instead of a password
 - “My dog’s first name is Rex”
 - problem: many sites/systems have a limit of characters
- Use the first letter of each word in a phrase
 - “My dog’s first name is Rex.” becomes “MdfniR”



Oregon State University
College of Engineering

USE STRONG PASSWORDS

Weak: Webster

Strong: W3b\$st3r

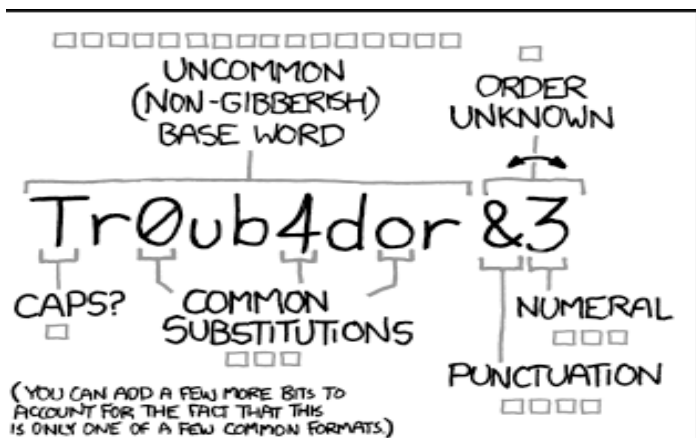
Stronger: A phras3 1s 3v3n StrOng3r!



SEL

ENGINEERING LABORATORIES, INC.

For information about cybersecurity solutions visit www.selinc.com/cybersecurity



~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□ □
□□□ □□□
□□□□ □


$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE
WEB SERVICE. YES, CRACKING A STOLEN
HASH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORRY ABOUT.)

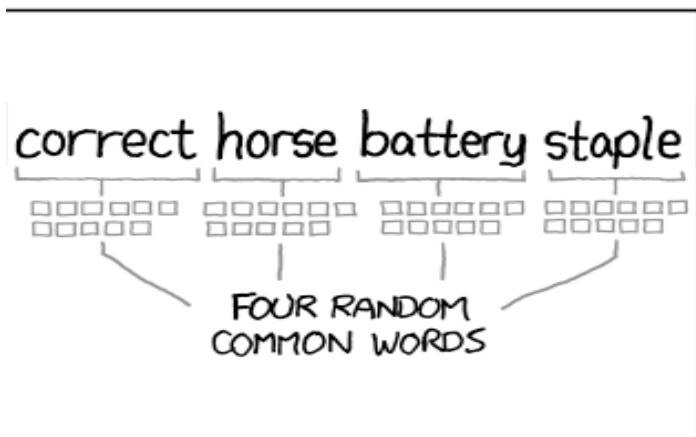
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

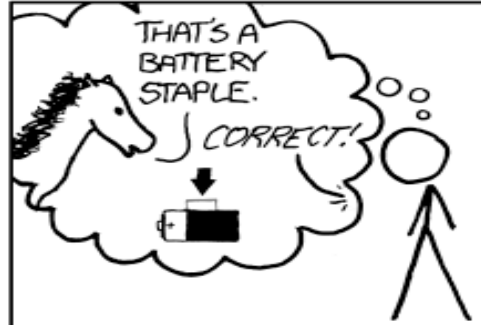
□□□□□□□□□□□□
□□□□□□□□□□□□
□□□□□□□□□□□□
□□□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A
BATTERY
STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

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.

Source: xkcd.com

#936

Calculating Password System Strength using Time



Oregon State University
College of Engineering

Anderson's formula:

- P probability of guessing a password in specified period of time of length T
- G number of guesses tested in 1 time unit
- T number of time units
- N number of possible passwords
- Then $P = (TG/N)$

Example



Oregon State University
College of Engineering

- Goal
 - Passwords drawn from a 96-char alphabet
 - Can test 10^4 guesses per second
 - Probability of a success to be no more than 0.5 over a 365 day period
 - What should be allowed password length?
- Solution
 - $N = TG/P = (365 \times 24 \times 60 \times 60) \times 10^4 / 0.5 = 6.31 \times 10^{11}$
 - Choose s such that $\sum_{j=0}^s 96^j \geq N$
 - So $s \geq 6$, meaning passwords should go up to 6 chars or more
 - What exactly does that equation mean?
 - Total # passwords using 96 chars, of length s or less

Anderson Formula Assumptions?

- Random password is picked
- Attacker is targeting a specific user account

Summary



Oregon State University
College of Engineering

- Passwords – “what you know” – authentication
 - Are widely used since the 60s
 - Easy to use and implement
- Password-based systems have vulnerabilities
 - Users tends to select weak passwords
 - Tension between memorability and strength
- Emerging approaches
 - Passphrases
 - System generated passwords



Oregon State
University

COLLEGE OF ENGINEERING

School of Electrical Engineering
and Computer Science

Password Based Authentication: Pros and Cons II

Password-based Authentication



Oregon State University
College of Engineering

- External entity is bound to system ID (user account)
- Authentication Step
 - External entity presents password
 - System compares with previously stored password
 - If password matches, system starts process with bound ID
- Later access control and privilege decisions made against ID

Password Systems - Advantages



Oregon State University
College of Engineering

- Password-based authentication has been around since 60s
 - It is widely used
- Why?
 - easy to implement
 - no special software needed on clients or servers
 - less expensive
 - no special hardware needed at the client side
 - easier to replace/recover
 - password reset (compare with tokens or biometrics)

Password Systems – Issues/Vulnerabilities



Oregon State University
College of Engineering

- Password Selection/Strength
- Password Storage
- Password Sharing/Re-use
- Social-engineering/Pre-texting
- Trusted Path/Electronic Monitoring
- System Design

Password Storage



Oregon State University
College of Engineering

- Store as cleartext
 - If password file compromised, *all* passwords revealed
- Encipher file
 - Need to have decipherment, encipherment keys in memory
 - Reduces to previous problem
- Store one-way hash of password
 - If file read, attacker must still guess passwords or invert the hash

Unix Password Hash Example



Oregon State University
College of Engineering

- Original UNIX system standard hash function
 - Hashes password into 13 character string
- As authentication system:
 - Authentication information is strings of 8 characters or fewer
 - System stores hash with user's identity in password file
 - Hash is complementation information
 - Verification function is hash on password and comparison with stored hash

Dictionary Attacks



Oregon State University
College of Engineering

- Trial-and-error from a list of potential passwords
 - *Off-line (type 1)*: know functions and registered information, and repeatedly try different guesses $g \in A$ until the list is done or passwords guessed
 - Examples: *crack*, *john-the-ripper*
 - *On-line (type 2)*: have access to verification functions. Try guesses until one succeeds.
 - Examples: trying to log in by guessing a password
 - True story : early authentication system, checked password character-by-character, flagged error *immediately* when 1st character not in password

Preventing Attacks



Oregon State University
College of Engineering

- Hide information so that either authentication input, authentication functions, or stored verification information cannot be found.
 - Example: UNIX/Linux shadow password files
 - Hides hashed passwords where only root has access
- Block access to all verification methods
 - Prevents attacker from knowing if guess succeeded
 - Example: preventing *any* logins to an account from a network
 - Prevents knowing results of verification function or accessing verification function.

Salting



Oregon State University
College of Engineering

- Have a set of n hash functions
 - Randomly select one function when registering new authentication info
 - Store ID of function with registered info
- When does this help? When does it not?

Examples



Oregon State University
College of Engineering

- Use salt as first part of input to hash function
- **Take-home message** --- use n extra bits independent of password to increase work needed by brute-force attack by up to 2^n

Reactive Password Checking



Oregon State University
College of Engineering

- Have a password cracking program running in the background
 - Shut down account of passwords it can crack
 - CPU intensive
 - Shutting down active accounts is likely to annoy someone important eventually.

Bloom Filter



Oregon State University
College of Engineering

Space efficient probabilistic data structure to tell whether a given element is a member of a set

- No false negatives
 - If an element is a member, then the bloom filter will not say it is not a member
- False positives are possible

Bloom Filter



Oregon State University
College of Engineering

Application – determine whether a password given at creation is one of a large list of easily cracked passwords

Bloom Filter

- Create N bit array
- Use k independent hash functions which hash into a space of 0 to $N-1$
- For each bad password bp ,
 - For every hash function h compute $h(bp)$ in $[0, N-1]$ and set the corresponding bit in the hash table
 - Each word marks up to k bits

Bloom Filter



Oregon State University
College of Engineering

- To check a password
 - Computer every version of the hash, and check the corresponding bits in the array
 - If all bits are 1, then the password is bad
- What about false positives?

Bloom Filter



Oregon State University
College of Engineering

- Assuming the k hash functions are truly independent, the probability of a given bit not being set to 1 by a randomly chosen word is $(1 - \frac{1}{N})^k$.
- After inserting B bad passwords, the probability of a given bit being still 0 is

$$\left(1 - \frac{1}{N}\right)^{kB}$$

so that the probability of it being 1 is

$$1 - \left(1 - \frac{1}{N}\right)^{kB}.$$

Choose a word not in the set, use the k hash functions, the probability of randomly hitting every bit set is the product

$$\left(1 - \left(1 - \frac{1}{N}\right)^{kB}\right)^k \approx (1 - e^{-kB/N})^k$$

Bloom Filter



Oregon State University
College of Engineering

Using previous expression you can answer questions such as

- For a given N (output width of a hash function) and B (size of bad password dictionary) how many hash functions (k) do I need to achieve a false positive probability less than p ?

Summary



Oregon State University
College of Engineering

- Passwords – “what you know” – authentication
 - Are widely used since the 60s
 - Easy to use and implement
- Password-bases systems have vulnerabilities
 - Passwords (or processed version) needs to be stored on server leading to offline/dictionary attacks
 - Online guessing attacks
 - Picking bad passwords
- Mitigation approaches
 - Reactive and proactive password checking



Password Based Authentication: Pros and Cons III

Password-based Authentication



Oregon State University
College of Engineering

- External entity is bound to system ID (user account)
- Authentication Step
 - External entity presents password
 - System compares with previously stored password
 - If password matches, system starts process with bound ID
- Later access control and privilege decisions made against ID

Password Systems - Advantages



Oregon State University
College of Engineering

- Password-based authentication has been around since 60s
 - It is widely used
- Why?
 - easy to implement
 - no special software needed on clients or servers
 - less expensive
 - no special hardware needed at the client side
 - easier to replace/recover
 - password reset (compare with tokens or biometrics)

Password Systems – Issues/Vulnerabilities



Oregon State University
College of Engineering

- Password Selection/Strength
- Password Storage
- Password Sharing/Re-use
- Social-engineering/Pre-texting
- Trusted Path/Electronic Monitoring
- System Design

Password Re-Use



Oregon State University
College of Engineering

- Estimated average number of account per person $\sim 19+$
 - Hard to remember infrequently used site passwords
- People tend to reuse a few passwords across many sites
- Maintenance crews re-use passwords across 100s of devices
 - e.g. pole-top devices
- Upside: convenience
- Downside:
 - impact of password compromise is higher
 - compromise of one site/device compromises other unrelated sites/devices

Password Re-Use



Oregon State University
College of Engineering

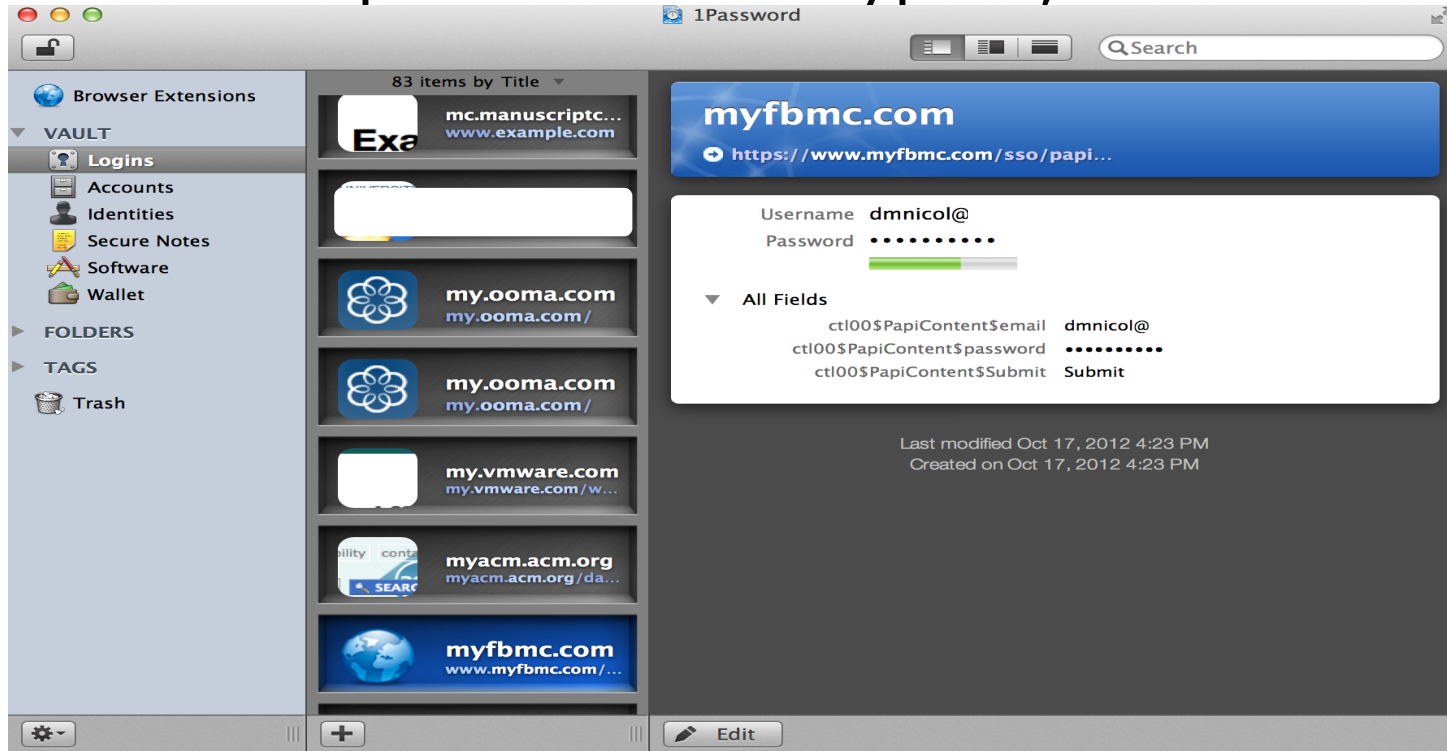
- Solution: Password manglers, Password managers, Single sign on
- Password Managers/Manglers
 - Used to be local and hard to carry with
 - Cloud computing changed that
 - Single point of failure
- Single Sign-On
 - Single point of failure

Example: 1Password



Oregon State University
College of Engineering

- Remembers passwords, can create them
- Bundle of passwords encrypted, stored in Dropbox



Password Sharing



Oregon State University
College of Engineering

- People share passwords
 - typically in single user systems used by many people
 - e.g., maintenance crew for pole-top devices
 - in families
- Upside: convenience
- Downside:
 - loss of accountability
 - higher risk for compromise

Social Engineering/Pre-texting



Oregon State University
College of Engineering

- Phishing e-mails
 - why is this possible or effective?
- Pre-texting
 - read the story on identity hacking

Trusted Path/Electronic Monitoring

- Spyware
 - False login screens
 - Ctrl-Alt-Del is meant to prevent that
- Keyboard loggers
- Fake windows/web-browsers

Password System Design



Oregon State University
College of Engineering

- Targeted account attack
- Targeted system attack
- Any account attack
- Denial of service

Summary



Oregon State University
College of Engineering

- Passwords – “what you know” – authentication
 - Are widely used since the 60s
 - Easy to use and implement
- Password-bases systems have vulnerabilities
 - Password sharing
 - Password re-use
 - Vulnerable to social engineering/pre-texting
 - Vulnerable to Trusted-path bugging
- Mitigation approaches
 - Single sign-on, password managers