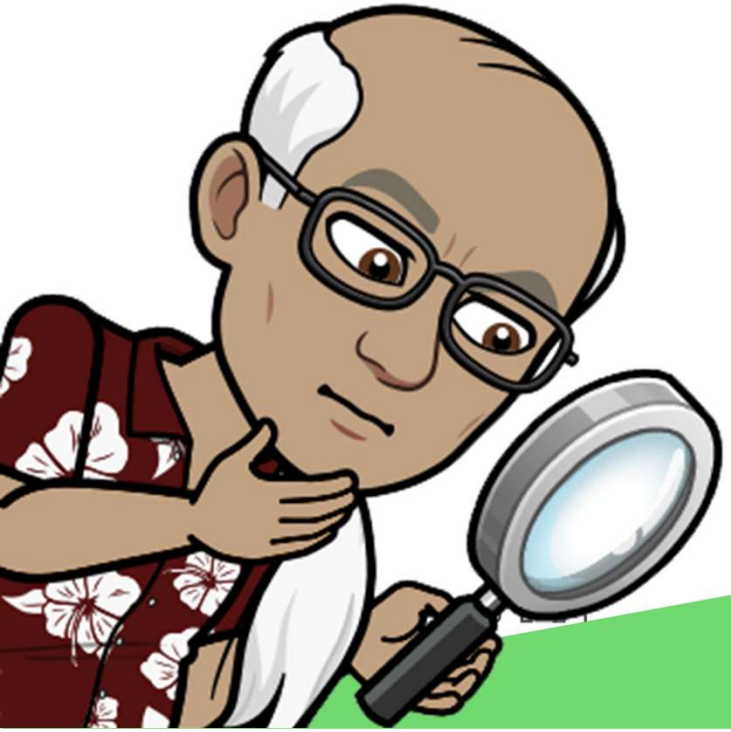
MODULE 2

Authentication

TECH ELEVATOR
A Stride Company

Authentication

- What is authentication?



Authentication is the process of verification that an individual, entity or website is who it claims to be.

Authentication is the front gate of any secure web application

Authentication Factors

something the user ***knows***

something the user ***has***

something the user ***is***

Authentication Factors

- the **knowledge factors**: Something the user knows (e.g., a password, Partial Password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern), Security question
- the **ownership factors**: Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)
- the **inherence factors**: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

Two-factor authentication

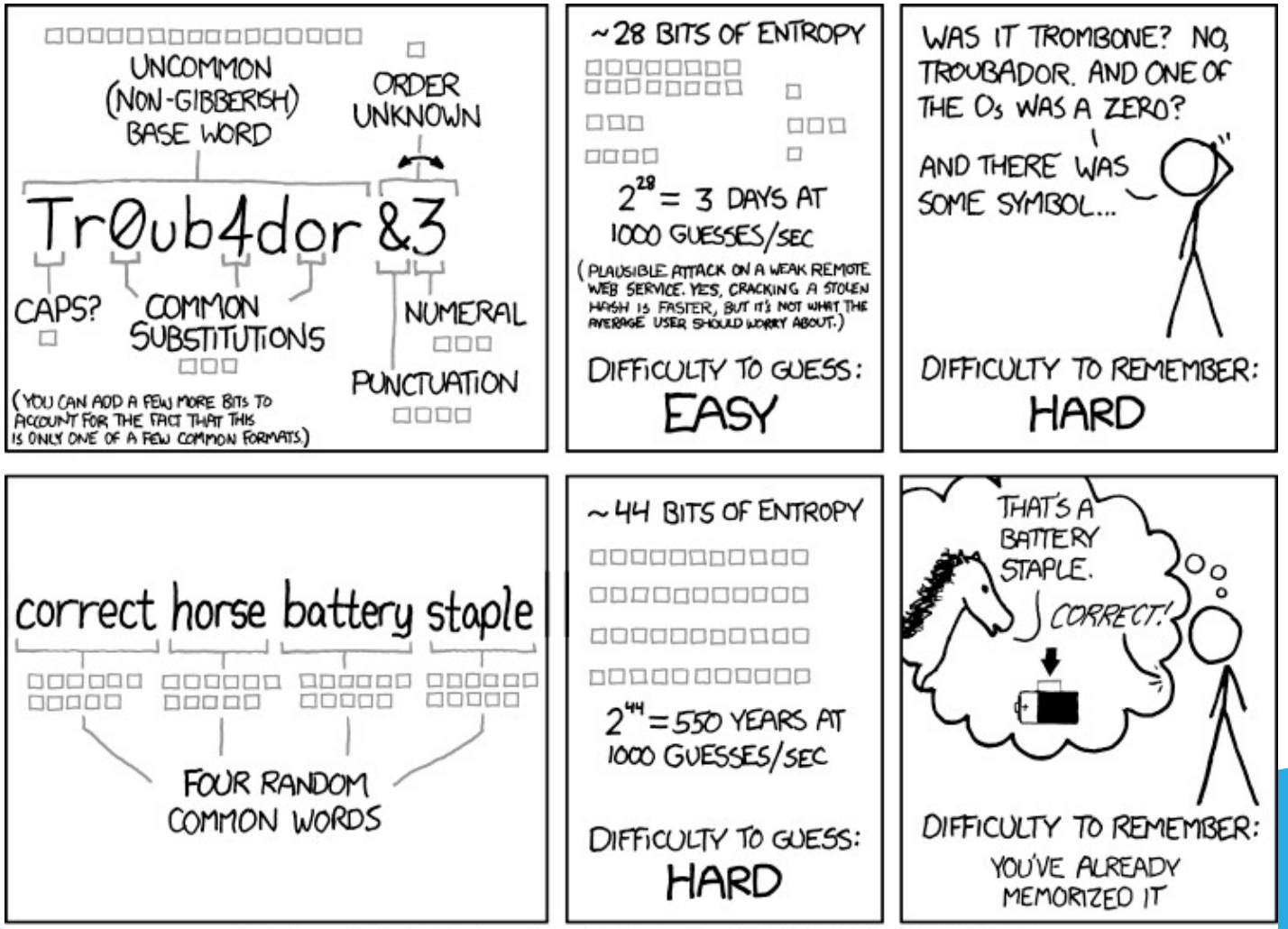
- a bankcard (something the user has) and a PIN (something the user knows).
- Business networks may require users to provide a password (knowledge factor) and a pseudorandom number from a security token (ownership factor).
- Apple requires developers to enter a password (something the user knows) and a pin sent to their registered phone (something the user has)

Passwords

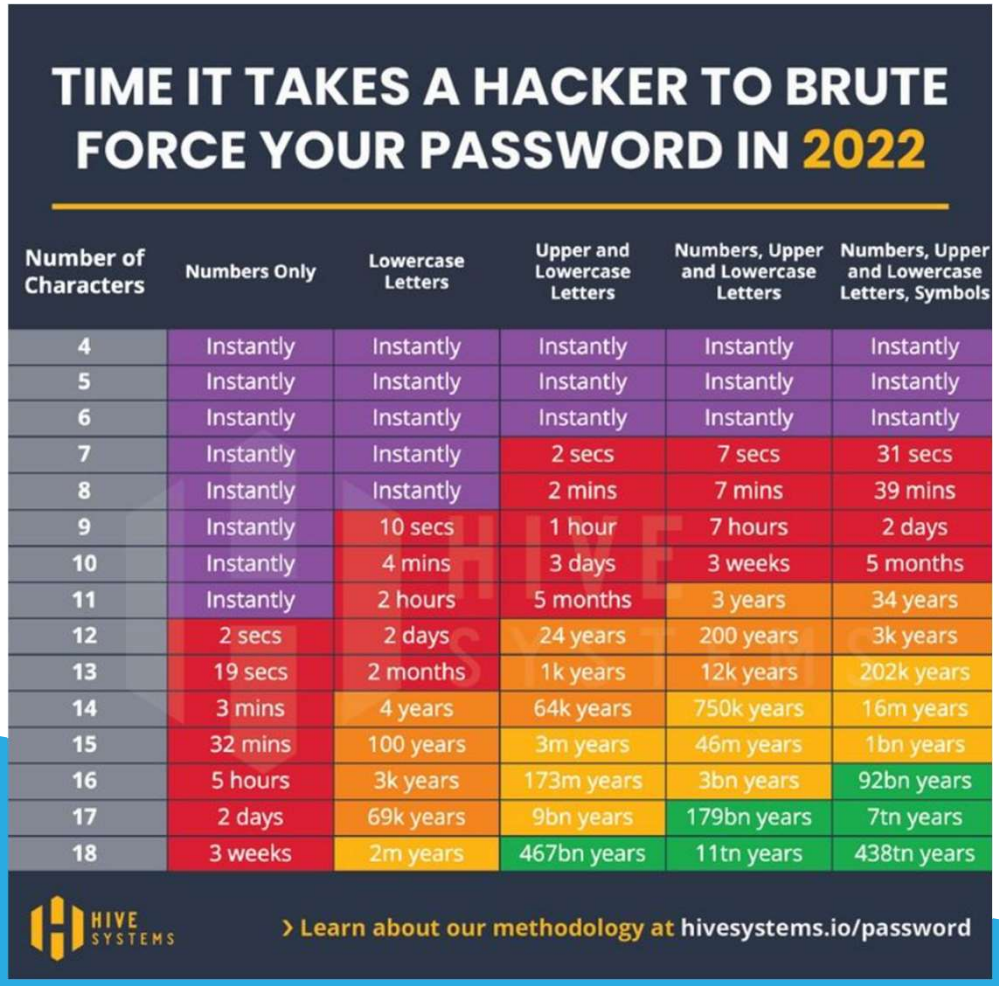
- The measure of password strength is called **Entropy.**
- Strong passwords have the following characteristics
  - Length: Passwords shorter than 10 characters are considered to be weak
  - Complexity: allow virtually any character and be case sensitive in order to increase their complexity

Password Policy

- Password must meet at least 3 out of the following 4 complexity rules
  - at least 1 uppercase character (A-Z)
  - at least 1 lowercase character (a-z)
  - at least 1 digit (0-9)
  - at least 1 special character (punctuation) — do not forget to treat space as special characters too
- at least 10 characters
- at most 128 characters
- not more than 2 identical characters in a row (e.g., 111 not allowed)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

Keeping the hounds at bay



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Authentication Beyond Password Rules

- Don’t tip your hand
  - Bad: The username is incorrect
  - Good: Login has failed

  - Bad: Invalid password
  - Good: Login has failed: Incorrect User Name or Password

- Make ‘em wait
  - Block log in attempts for 20 minutes if 5 failed attempts
  - Each failed attempt takes longer and longer to return an error

- Log them out if idle
  - Session timeouts to prevent session hijacking.

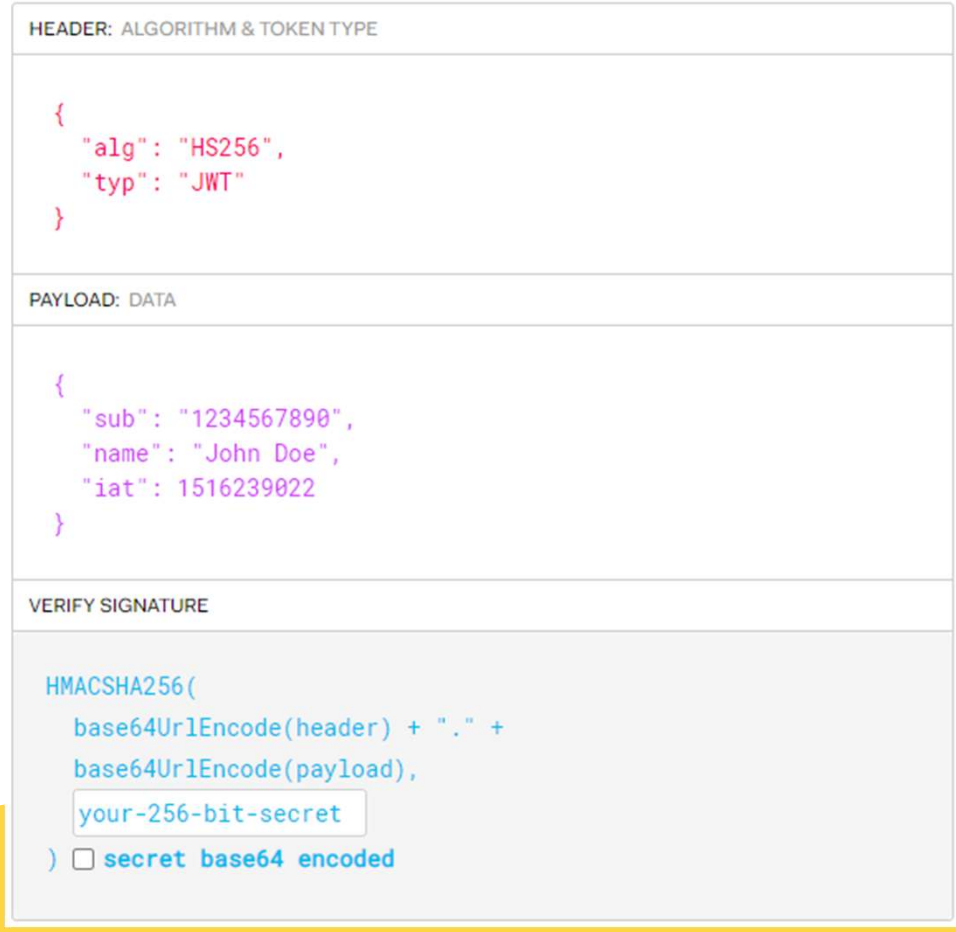
Mechanics of Authentication

- Ask user for username and password
- Verify the user has provided the proper credentials
- Keep tabs that they are authenticated

JSON Web Tokens (JWT)

eyJhbGciOiJIUzI1NiIsInR5cCI6Ik
pXVCJ9.eyJzdWIiOiIxMjM0NTY3O
DkwIiwibmFtZSI6IkpvaG4gRG9lIi
wiaWF0IjoxNTE2MjM5MDIyfQ.Sfl
KxwRJSMeKKF2QT4fwpMeJf36P
Ok6yJV_adQssw5c

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.



ELEVATE YOURSELF

JWT Highlights

- Their compact size allows for quick transfer with requests.
- They're often used as authorization mechanisms, storing user info such as their permissions or roles. These are called "claims."
  - They can contain any data that can be represented in JSON.
- JWT actually contains JSON, but it's encoded.
- Integrated for claims base security

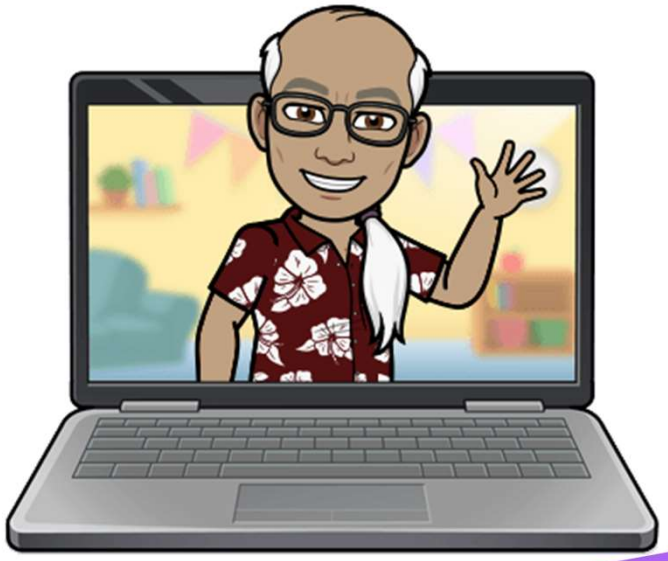
Things for the Server

- @PreAuthorize(“isAuthenticated()”)
- @PreAuthorize(“hasRole(‘admin’)”)
- @PreAuthorize(“hasAnyRole(‘admin’,’student’)”)
- @PreAuthorize(“isAnonymous()”)
- @PreAuthorize(“permitAll”)

Getting the Current User

```
@PreAuthorize("hasRole('ADMIN')")
@ResponseStatus(HttpStatus.NO_CONTENT)
@RequestMapping(path = "/reservations/{id}", method = RequestMethod.DELETE)
public void delete(@PathVariable int id, Principal principal) throws ReservationNotFoundException {
   auditLog("delete",id,principal.getName());
   reservationDao.delete(id);
}
```

LET’S CODE!



WHAT QUESTIONS DO YOU HAVE?

Reading for tonight: