JÖNKÖPING UNIVERSITY

School of Engineering

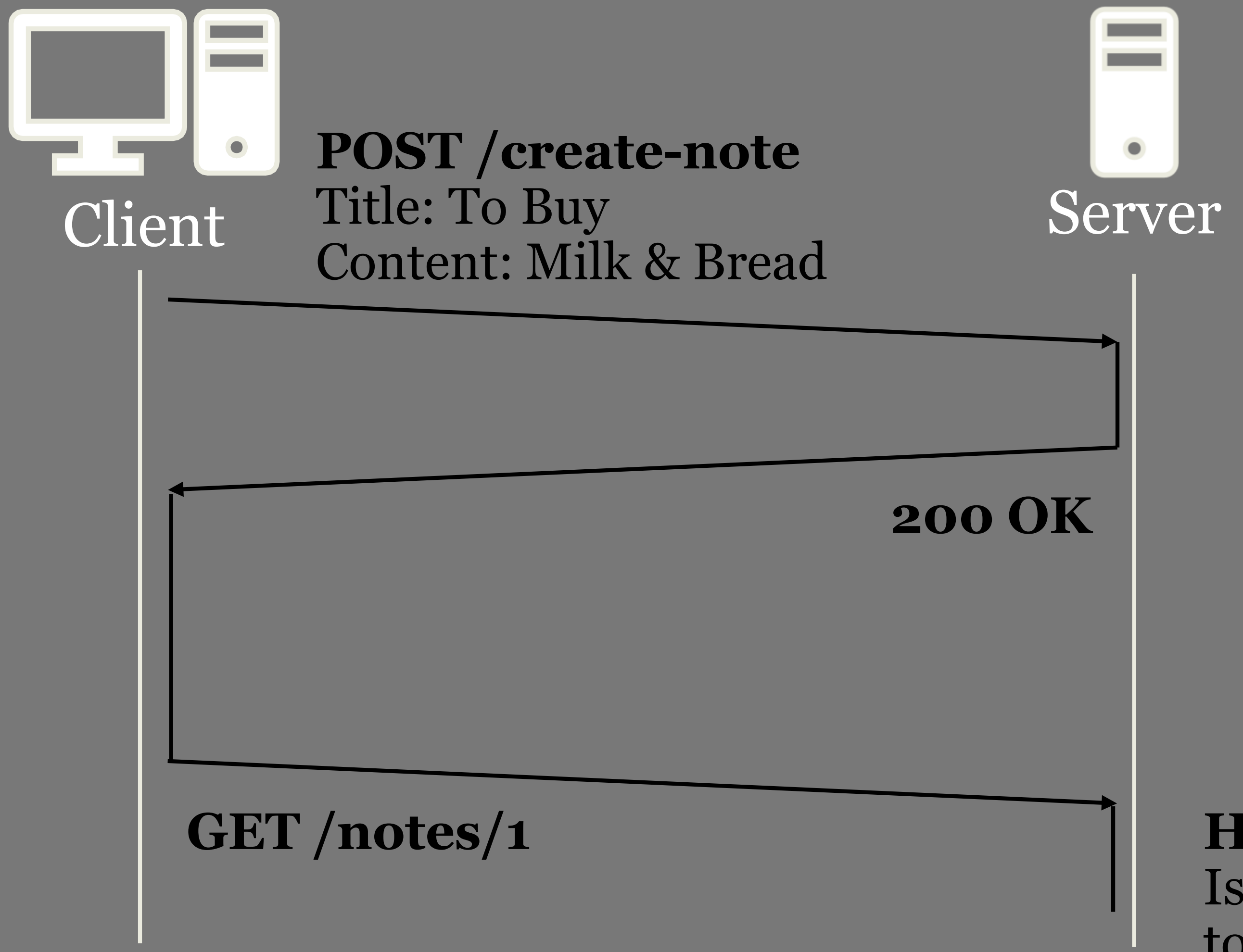
DESIGNING ACCOUNT SYSTEMS

Peter Larsson-Green

Jönköping University

Autumn 2018

AUTHORIZATION



POST /create-note
Title: To Buy
Content: Milk & Bread

200 OK

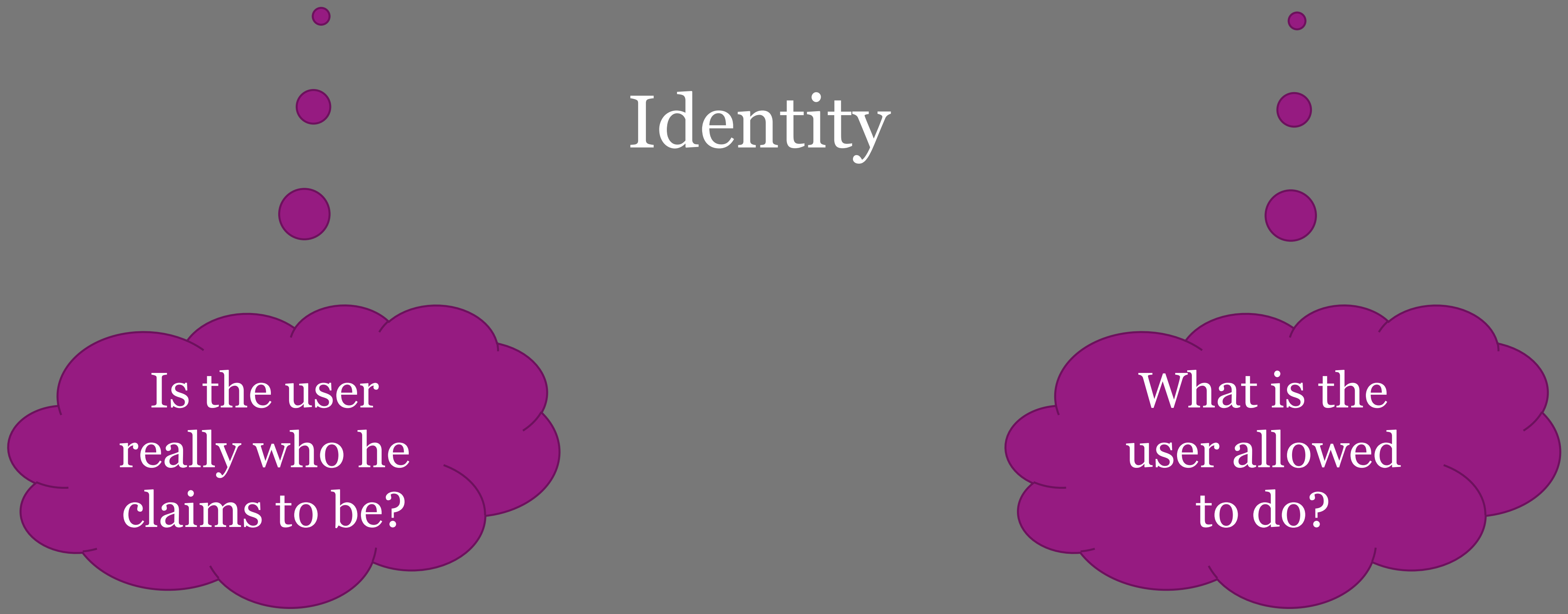
GET /notes/1

Notes

Id	Title	Content
1	To Buy	Milk & Bread

Hmm…
Is she authorized
to request that?

AUTHENTICATION & AUTHORIZATION

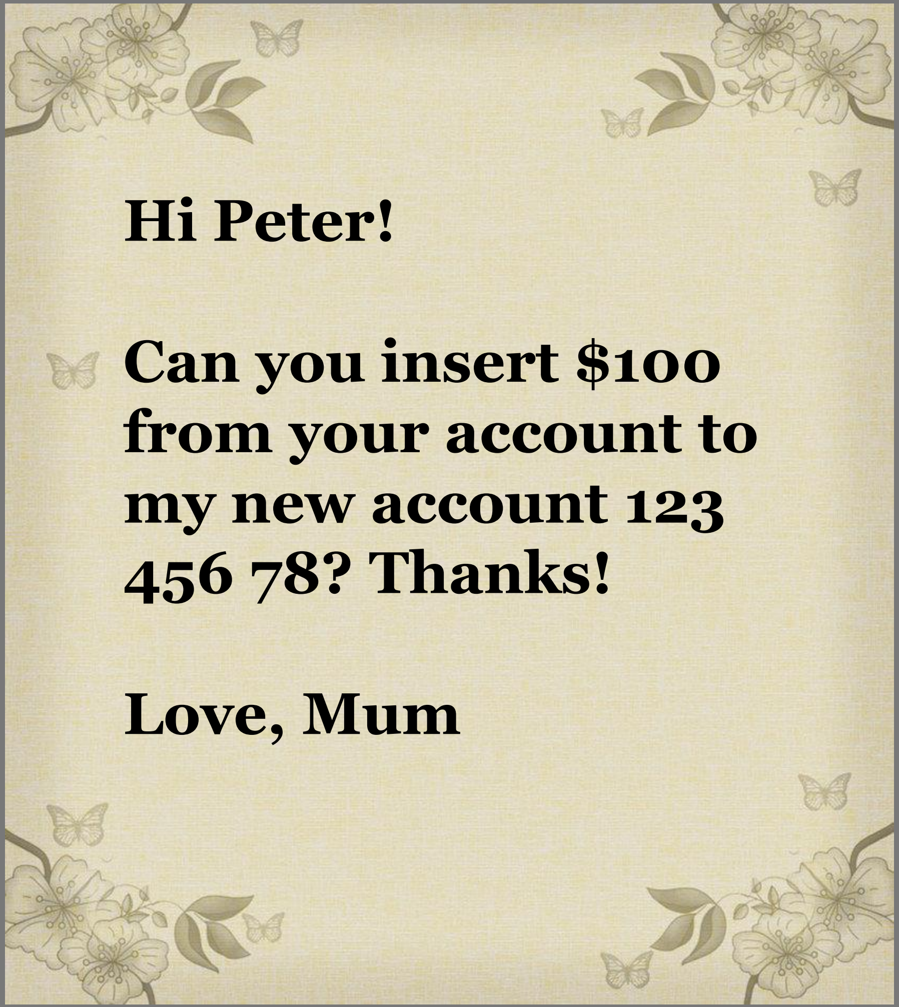


Identity

Is the user really who he claims to be?

What is the user allowed to do?

COMPARING TO REAL LIFE



Hi Peter!

Can you insert $100 from your account to my new account 123 456 78? Thanks!

Love, Mum

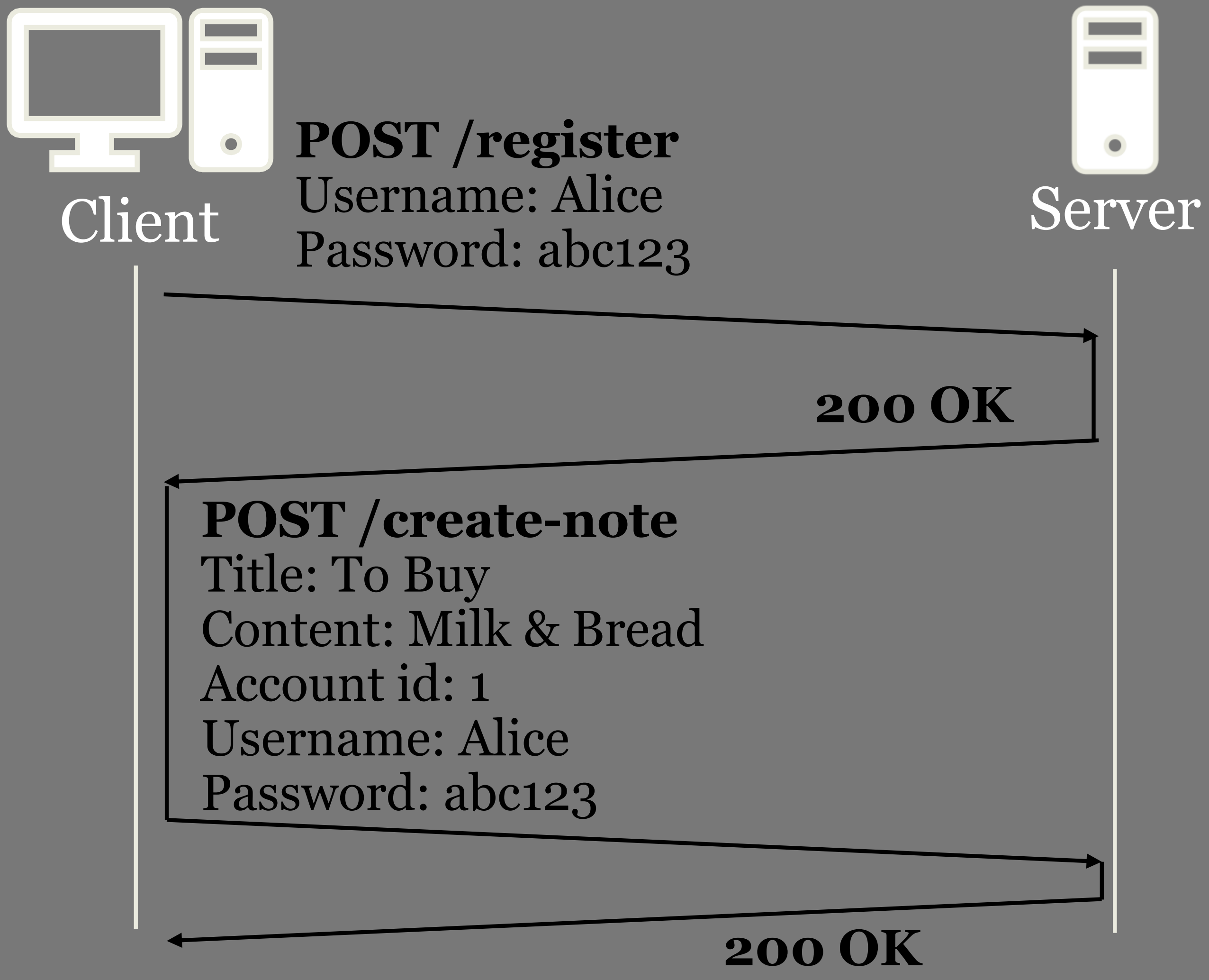
IMPLEMENTING AUTHENTICATION

1. Users needs to be uniquely identified.
   - Use account resources.
2. Users needs to be able to prove ownership of an account.
   - Each user shares a secret with the server, e.g. a password.

Accounts

Id	Username	Password
1	User A	Password A
2	User B	Password B
3	User C	Password C
4	User D	Password D

AUTHORIZATION WITH AUTHENTICATION



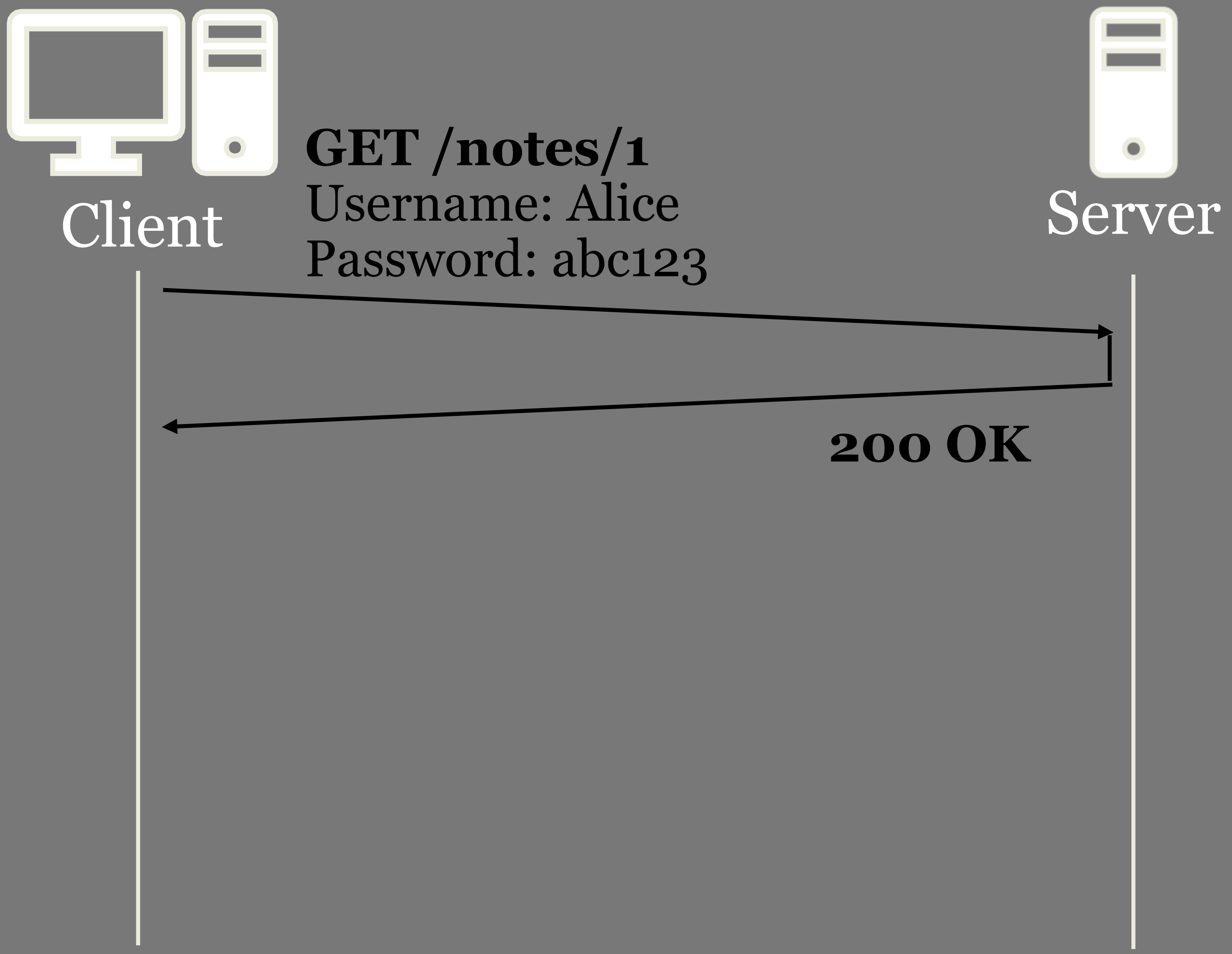
Accounts

Id	Username	Password
1	Alice	abc123

Notes

Id	AccountId	Title	Content
1	1	To Buy	Milk & Bread

AUTHORIZATION WITH AUTHENTICATION



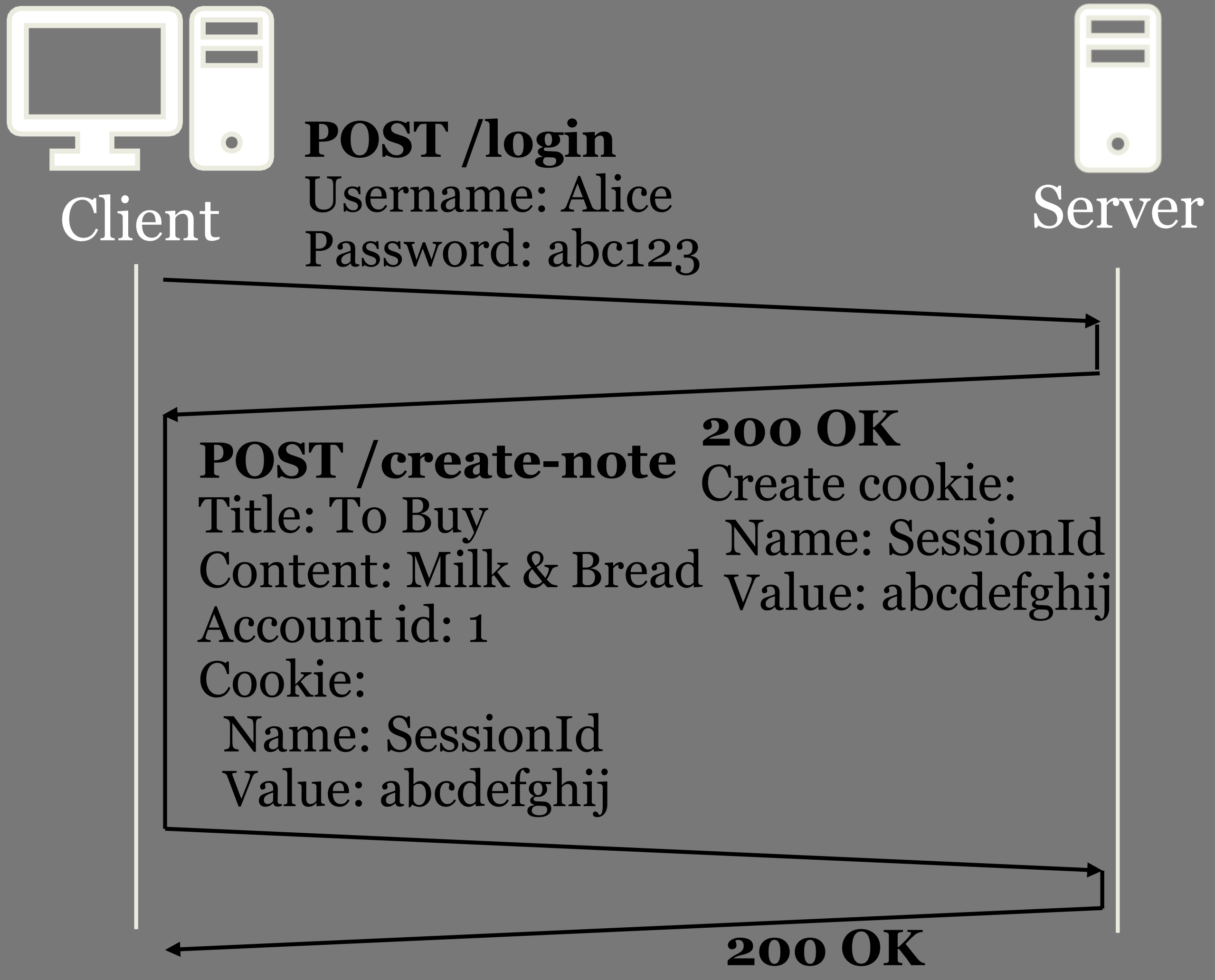
Accounts

Id	Username	Password
1	Alice	abc123

Notes

Id	AccountId	Title	Content
1	1	To Buy	Milk & Bread

AUTHORIZATION WITH SESSIONS



POST /login
Username: Alice
Password: abc123

200 OK
Create cookie:
Name: SessionId
Value: abcdefghij

POST /create-note
Title: To Buy
Content: Milk & Bread
Account id: 1
Cookie:
Name: SessionId
Value: abcdefghij

200 OK

Accounts

Id	Username	Password
1	Alice	abc123

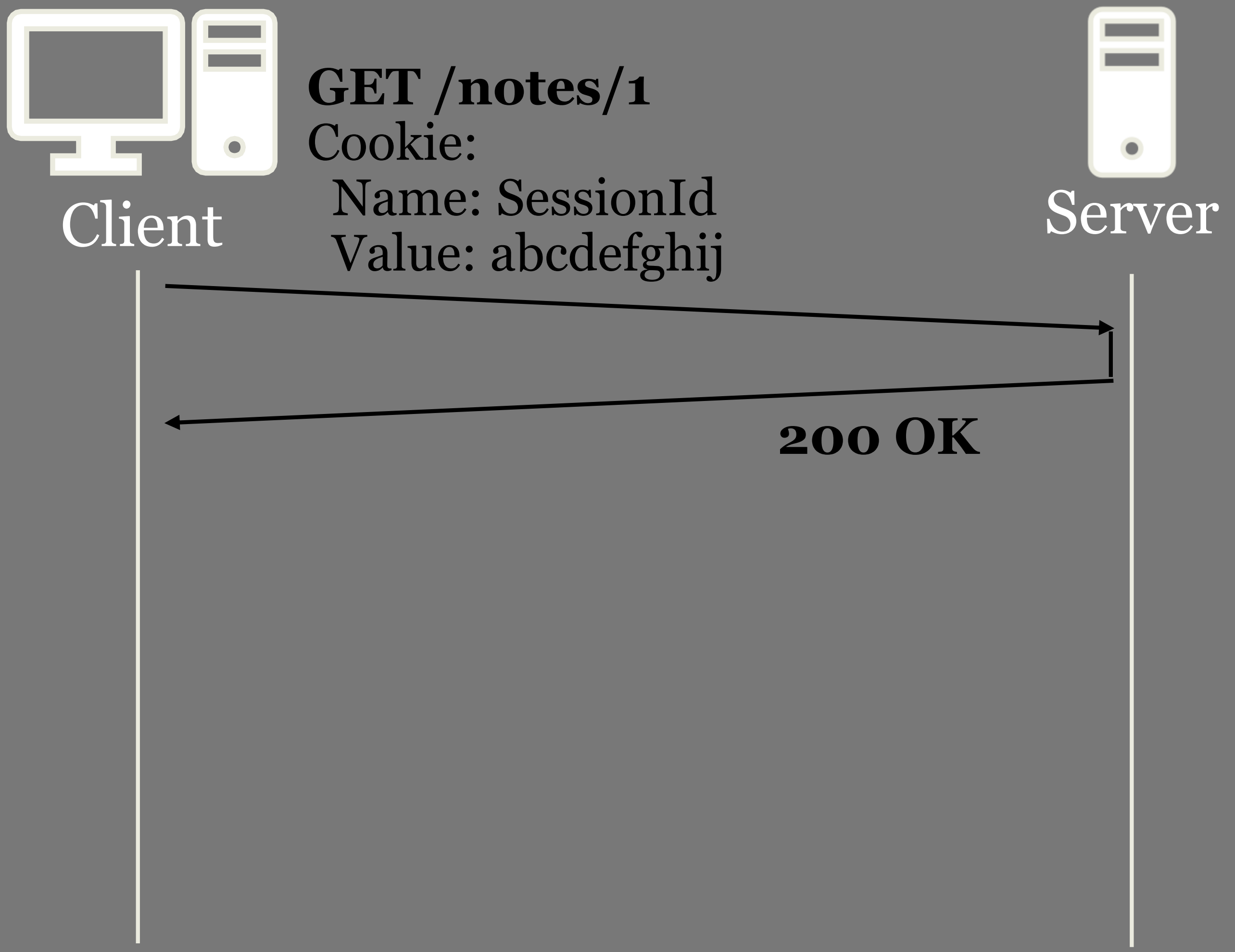
Sessions

Id	AccountId
abcdefghij	1

Notes

Id	AccountId	Title	Content
1	1	To Buy	Milk & Bread

AUTHORIZATION WITH SESSIONS



Accounts

Id	Username	Password
1	Alice	abc123

Sessions

Id	AccountId
abcdefghij	1

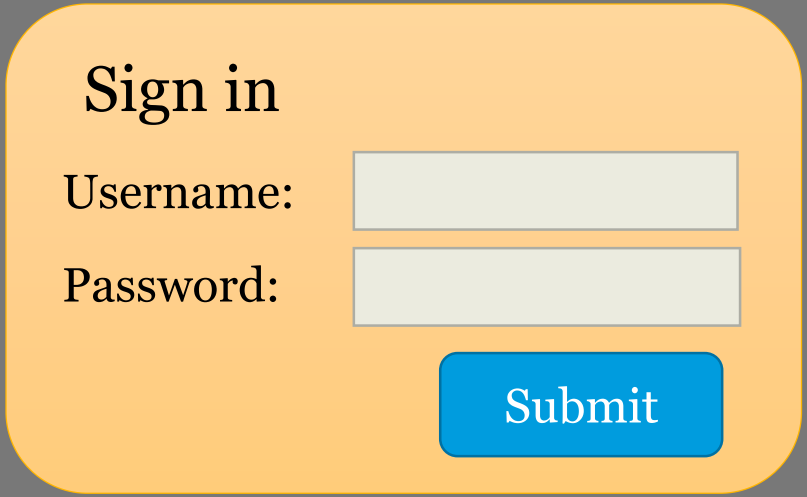
Notes

Id	AccountId	Title	Content
1	1	To Buy	Milk & Bread

SIGN IN AS SOMEONE ELSE

Accounts

Username	Password
Lisa	jklSD$2Fk3
Bart	123456
Homer	1+4=8
Marge	ilovehs



Sign in

Username:

Password:

What do the hacker do?

Keeps trying different passwords until he successfully logins.

What can we do?

Limit the number of login attempts.

IF WE ARE HACKED

Accounts

Username	Password
Lisa	jklSD$2Fk3
Bart	123456
Homer	1+4=8
Marge	ilovehs

What do the hacker do?

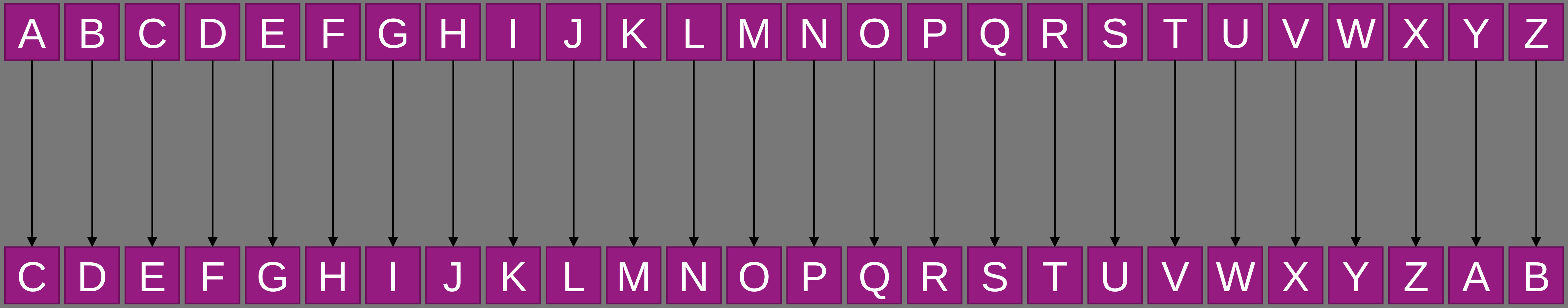
Logins as the users on other websites.

What can we do?

Don't store the passwords in plaintext.

ENCRYPTION

Caesar cipher
Key = 2



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

When the user signs up:

Store the password encrypted.

Username	Password
Stupid	SIMPLE

When the user signs in:

Decrypt the encrypted password and compare it with the provided one.

Username	Encrypted Password
Stupid	UKORNG

IF WE ARE HACKED

The hacker can't read the passwords in plain text ☺

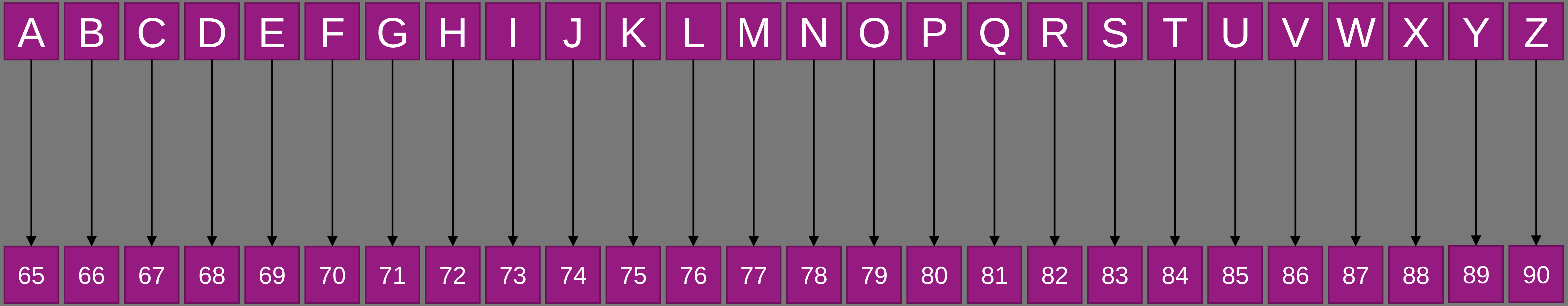
What do the hacker do?

Searches for the encryption function and decrypts the encrypted passwords.

What do we do?

Hash the passwords instead of encrypting them.

HASHING (MUL + MOD)



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

When the user signs up:

Store the hash of the password.

Username	Password
Stupid	SIMPLE

When the user signs in:

Hash the provided password and compare it with the stored hash.

Username	Hashed Password
Stupid	83*73*77*80*76*69 % 1000 = 360

IF WE ARE HACKED

Username	Hashed Password
Stupid	360

The hacker can't read the password in plaintext ☺

The hacker can't "unhash" the hashed passwords ☺

Rainbow Table

Plain text	Hashed
password	746
123456	254
qwerty	968
simple	360
aaaaaa	173

What do the hacker do?

Uses rainbow tables with common passwords to "unhash" the hash.

What do we do?

Add static salt to the password we hash.

```
hash("theSalt"+"thePassword")
```

IF WE ARE HACKED

What do the hacker do?

Creates his own rainbow table with the same salt.

Rainbow Table

Plain text	Hashed
theSaltpassword	245
theSalt123456	587
theSaltqwerty	163
theSaltsimple	93
theSaltaaaaaa	974

What do we do?

Use dynamic salt instead (each user has its own salt).

Username	Salt	Hashed Password
Stupid	ksjktjf	215
Member X	lkdyrar	722
Member Y	jskdjtny	859

The hacker needs to generate one rainbow table for each user
→ Takes time ☺

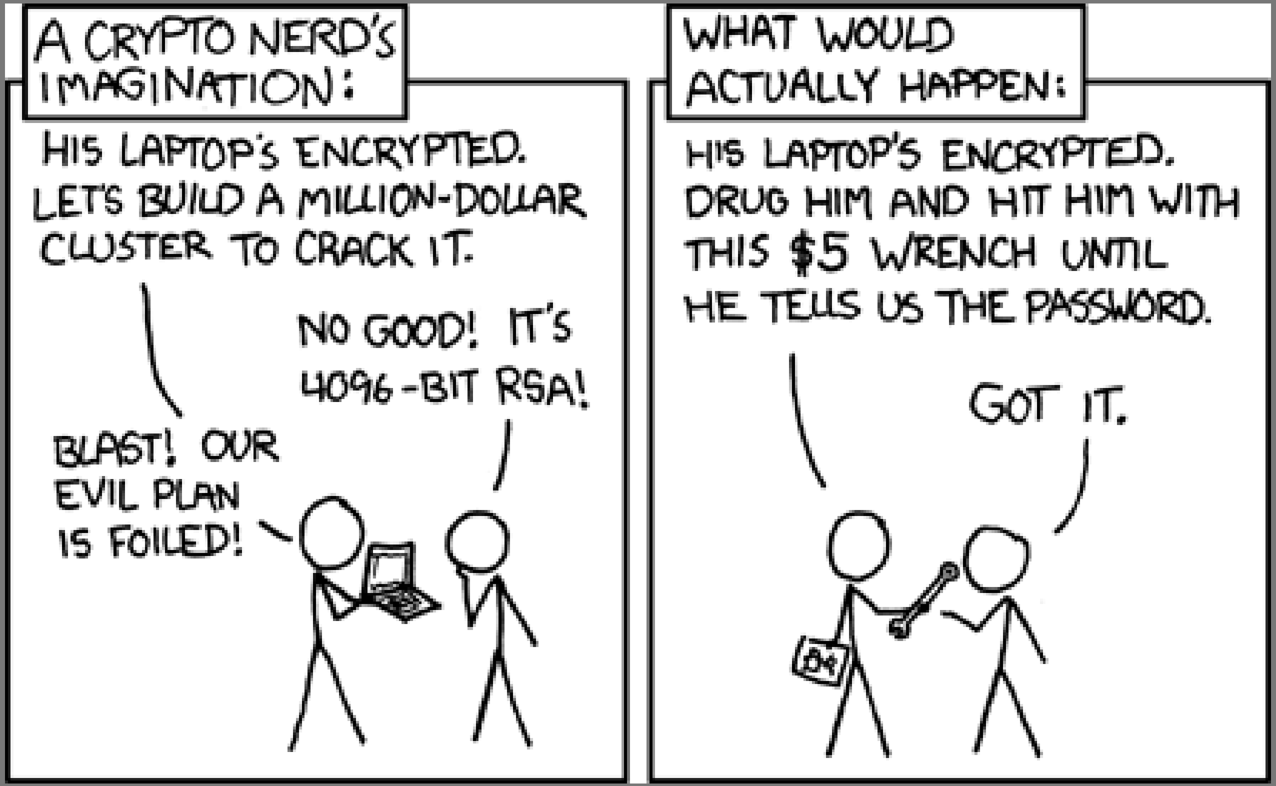
WHAT MORE CAN WE DO?

- Only short and common passwords are risky.
  - Use a minimum length for passwords.
  - Only accepts passwords containing both lower and upper case letters as well as symbols and digits.
- But it's hard to remember long random passwords.
  - Humans choose simple ones (`He||0W0r1d`) ☹

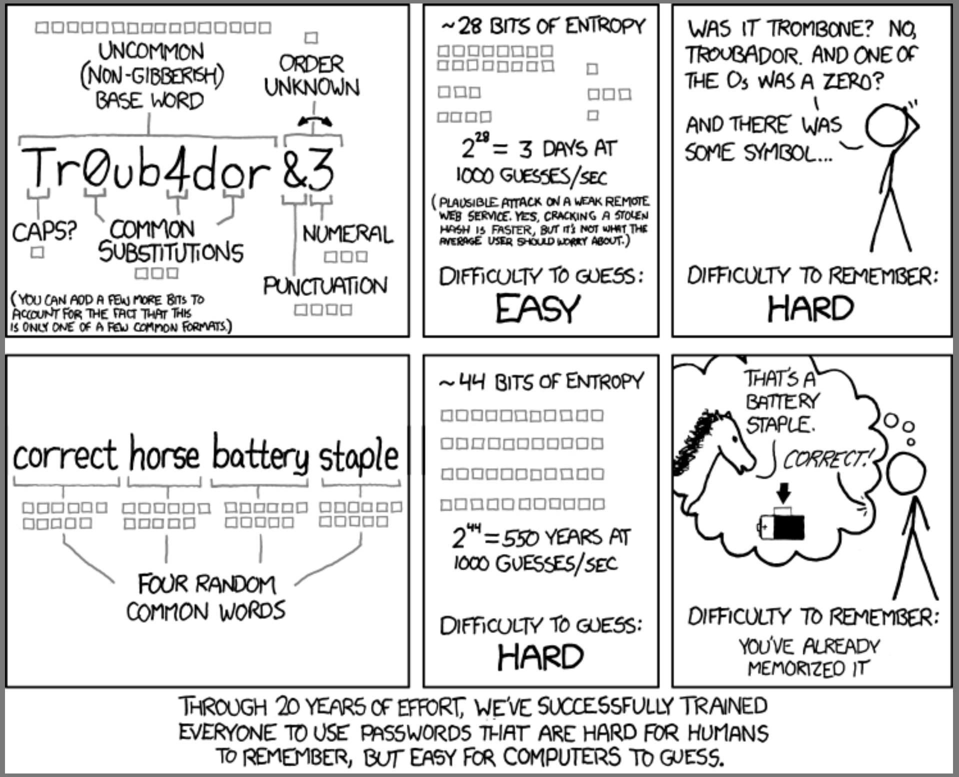
FUN OF THE DAY

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

FUN OF THE DAY


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
$4

https://xkcd.com/538/


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.

https://xkcd.com/936/