

COMP435: *SECURITY CONCEPTS!*

Lecture 4: User Authentication

tinyurl.com/comp435-fa25



USER AUTHENTICATION



User Authentication

System



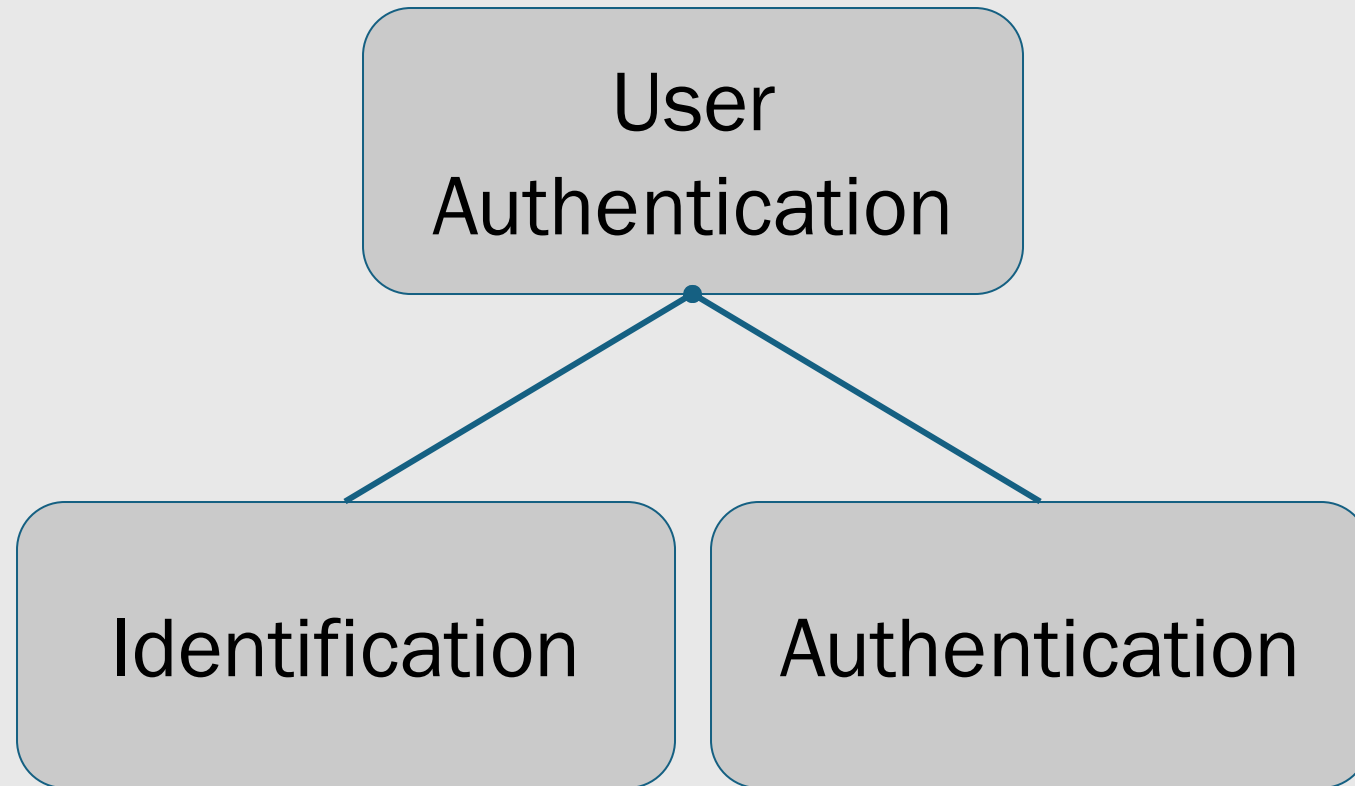
Policy

May Enter

+ family
members
+ friends

May Not Enter

- everyone else



Identification

Def'n: Asserting who a person is

E.g., “Hello, my name is Kaki”

Implicit



Explicit



Authentication

Def'n: Proving an asserted identity

E.g., *shows driver's license*

STATE ISSUED ID



STUDENT ID



Identification

- public
- well known

Authentication

- private
- unforgeable
- authentic

Means of Authentication

Which of the following is NOT a means of authenticating a user's identity?

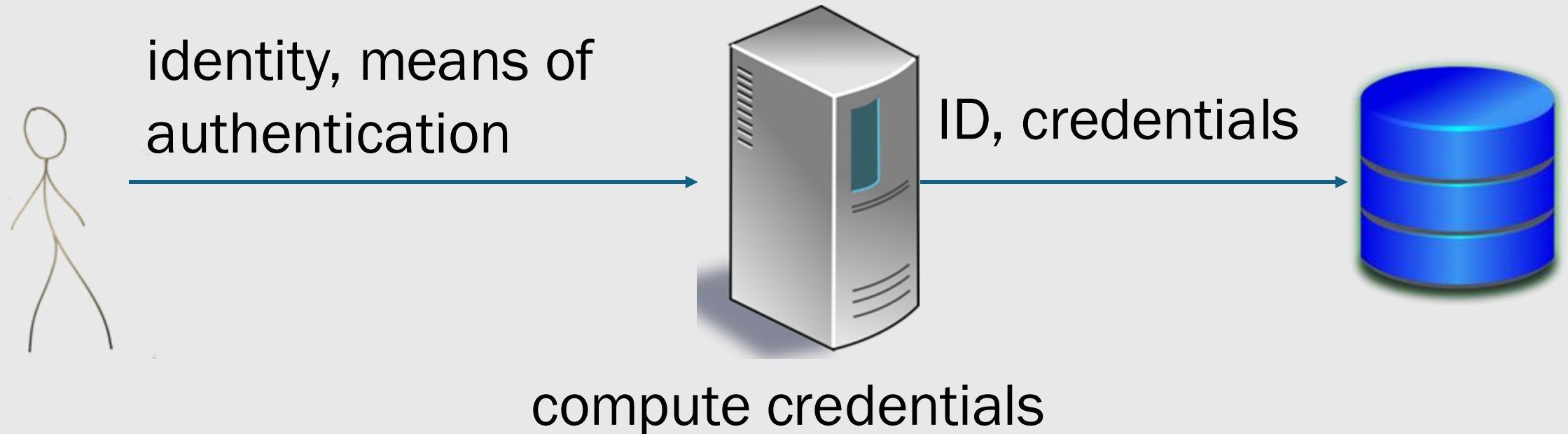
1. Drivers license
2. Passport
3. Door key
4. A name tag



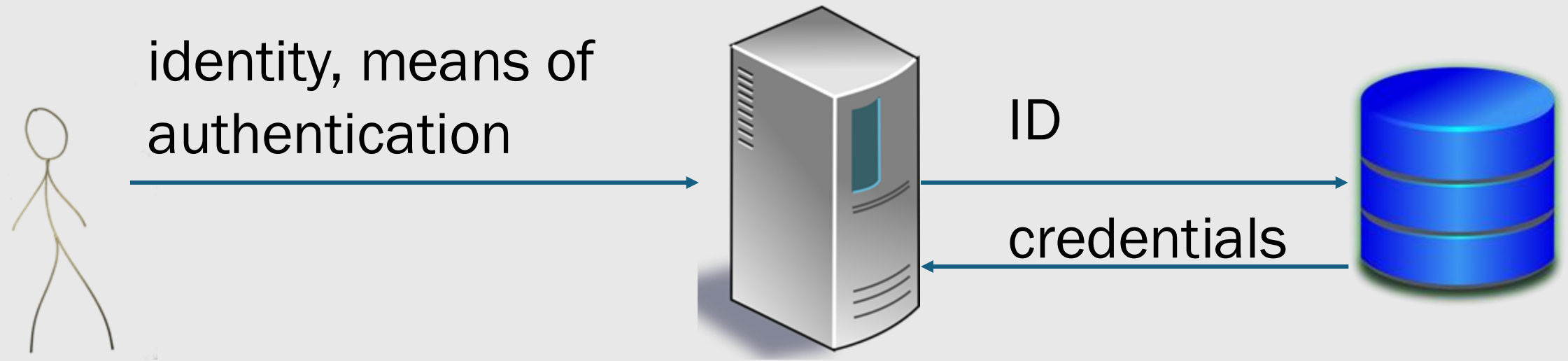
USER AUTHENTICATION... IN COMPUTER SYSTEMS!



Registration



Authentication



1. compute credentials
2. comparison

Means of Authentication

What you
know

What you do
or what you
are

What you
have

Where you
are



PASSWORDS



Means of Authentication

What you
know

What you do
or what you
are

What you
have

Where you
are

passwords

Passwords



- Ubiquitous
- Easy to use
- No extra hardware

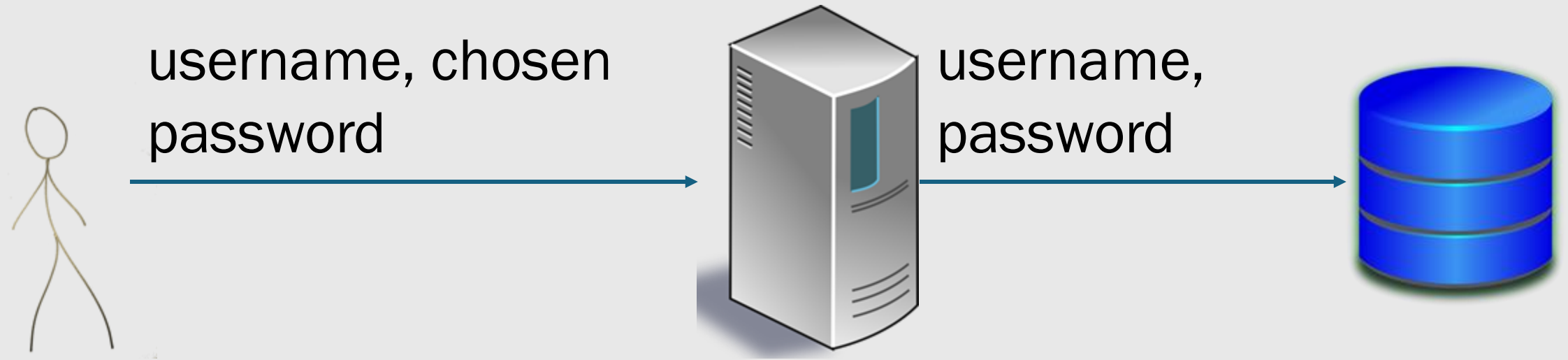
Pros



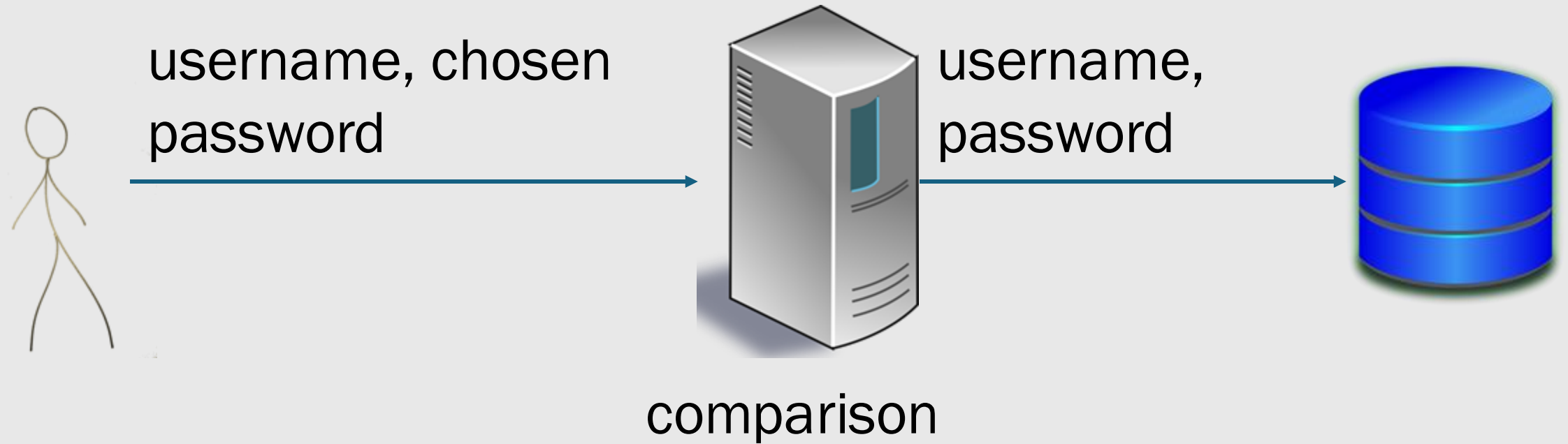
- Easy to attack
- Difficult to use well

Cons

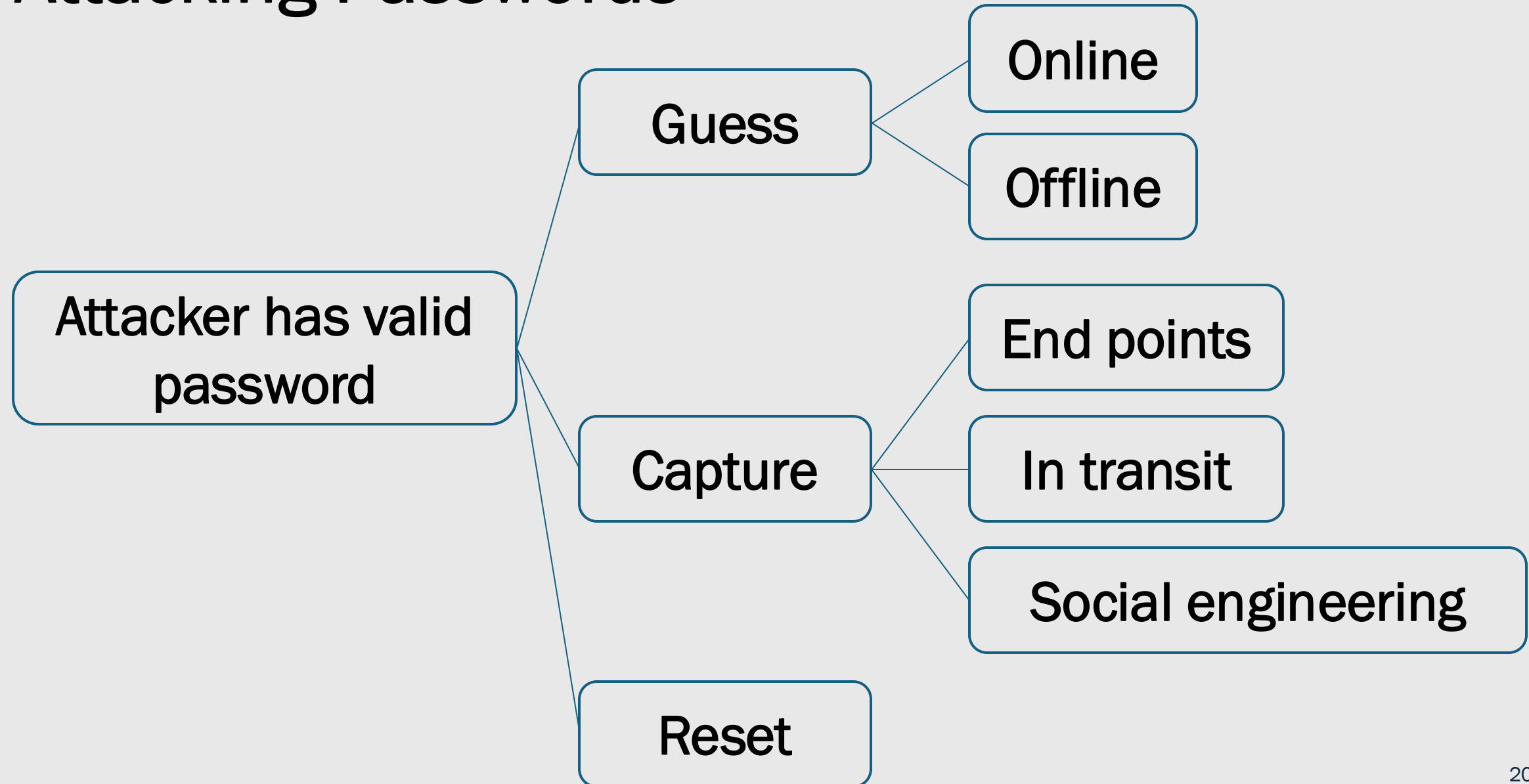
Registration



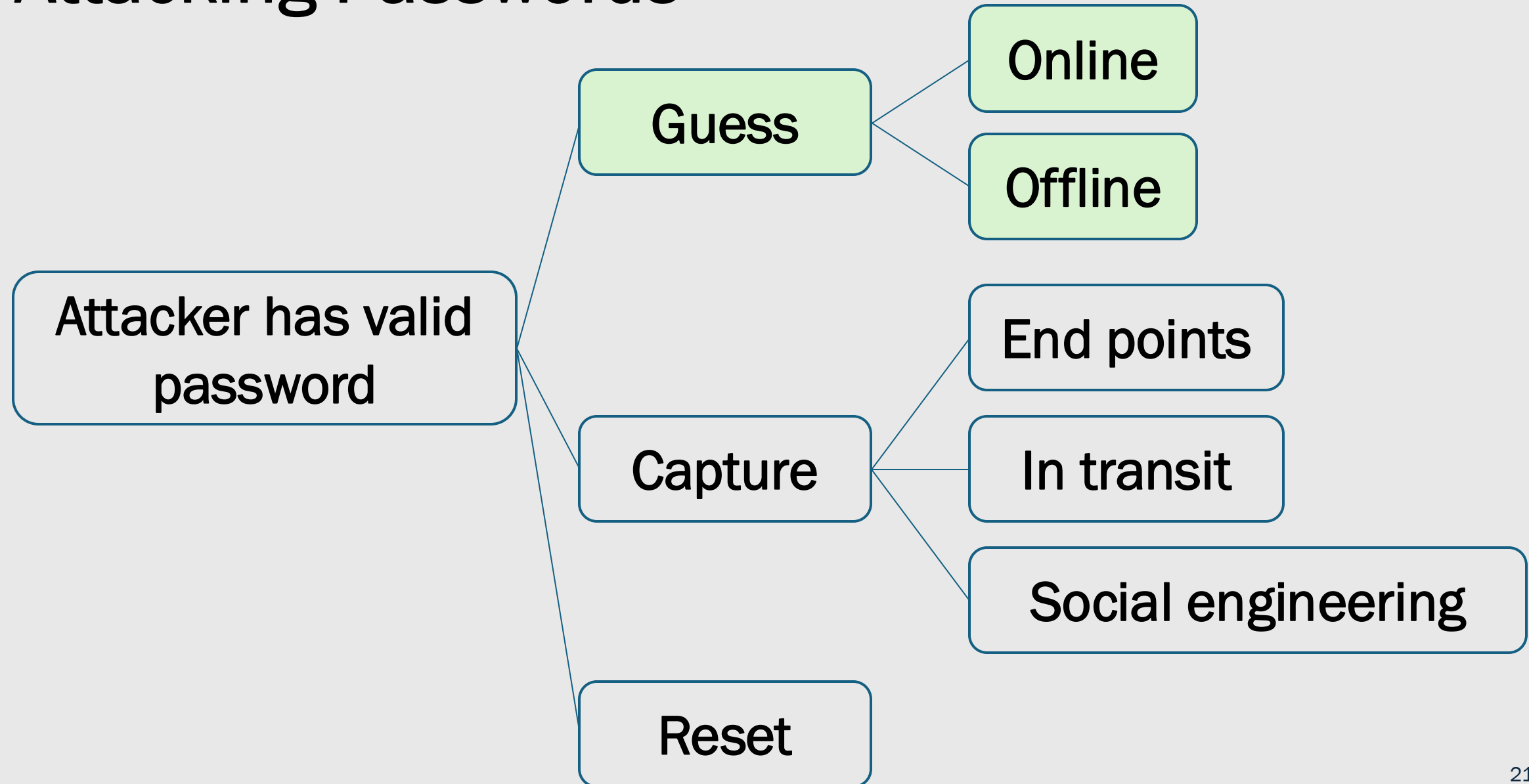
Authentication



Attacking Passwords



Attacking Passwords



What is the attacker's chance of guessing correctly?

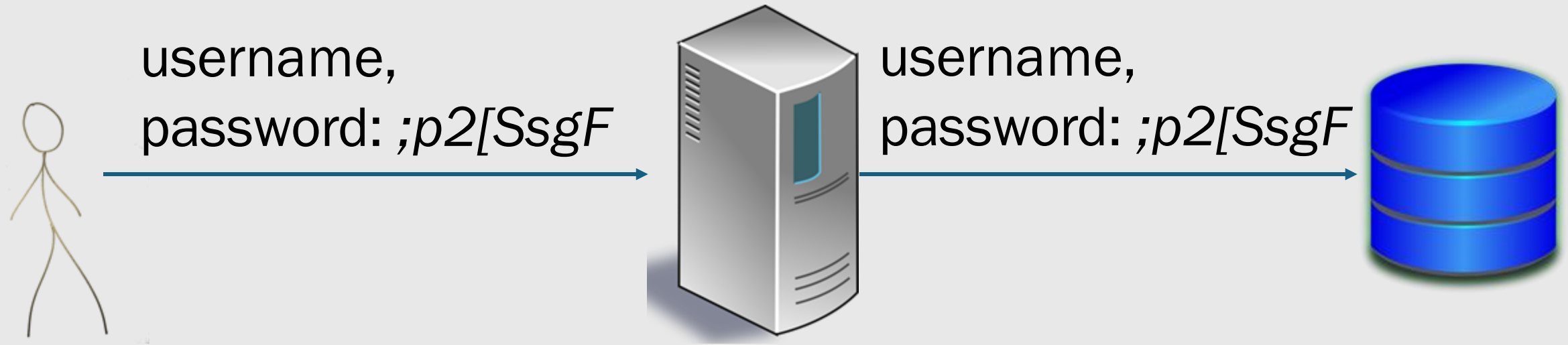
8-character passwords

printable characters (excluding space)

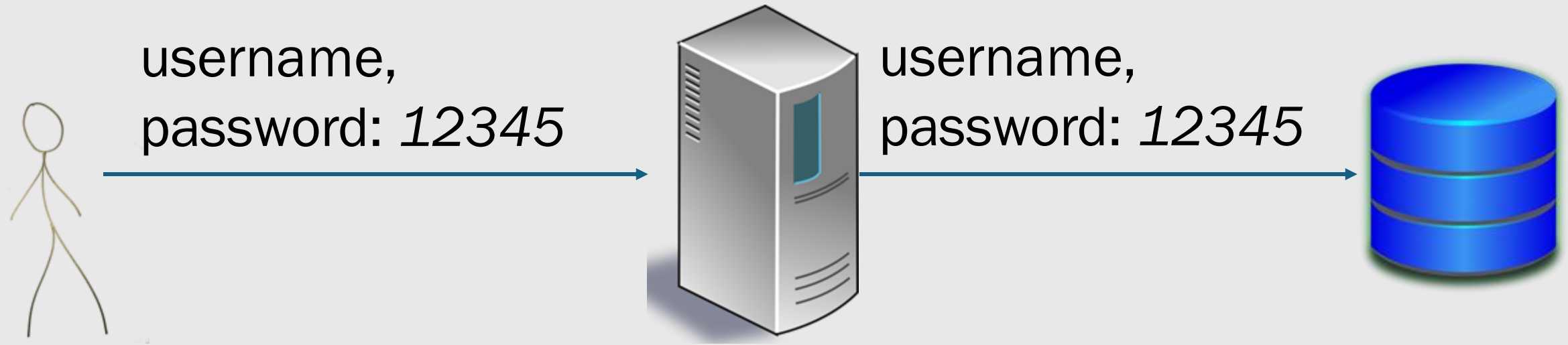
- *52 alphabetic*
- *10 numeric*
- *32 add'l (excluding space)*

If there are 2^{53} possible passwords, how long will it take, on average, for the attacker to guess the right one assuming the attacker can try **10,000 passwords per second**

Registration



Registration



Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions

Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



learnable online,
small set

Common Passwords


- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



600,000 English
words

Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



e:3, o:0, t:7,
l:1, for:4



ONLINE GUESSING ATTACKS



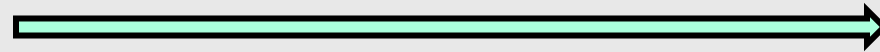
Attacker



Resource



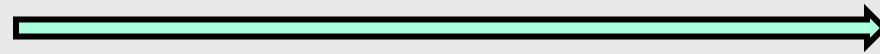
alice, 1234



access denied



alice, qwerty



Targeted Attack

Def'n: an attack aimed at a specific user

Targeted Attack



guess common
passwords



Identity	Password
Jane	p2ssw0rd!
Patrick	qwerty
Philip	ilovefido
Roz	qwerty
Claire	aq3wm\$oTo!4

Targeted Attack



guess common
passwords



use personal
information



Identity	Password
Jane	p2ssw0rd!
Patrick	qwerty
Philip	ilovefido
Roz	qwerty
Claire	aq3wm\$0To!4

Targeted Attack

guess common
passwords

use personal
information

Countermeasure:
rate-limit guesses

Trawling Attack

Def'n: an attack that tries to gain access to a system through any of its users.

Trawling Attack

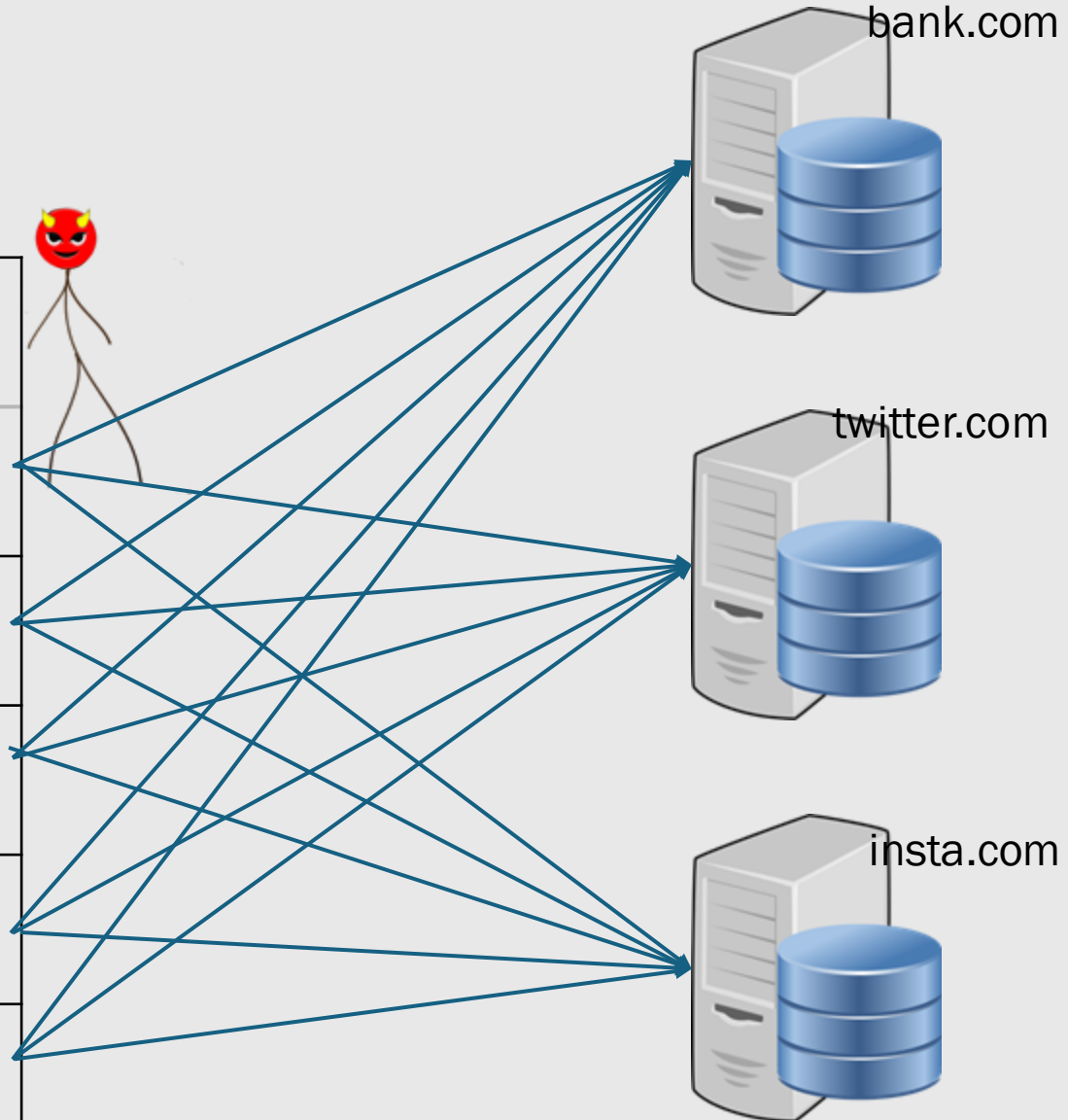


guess common
passwords against
many users

Identity	Password
Jane	p2ssw0rd!
Patrick	qwerty
Philip	ilovefido
Roz	qwerty
Claire	aq3wm\$0To!4

Credential Stuffing Attack

Identity	Password
Jane	p2ssw0rd!
Patrick	qwerty
Philip	ilovefido
Roz	qwerty
Claire	aq3wm\$oTo!4





OFFLINE GUESSING ATTACKS



Identity	Password
Jane	p2ssw0rd!
Patrick	qwerty
Philip	ilovefido
Roz	qwerty
Claire	aq3wm\$0To!4



Defense: Hashed Passwords

Identity	h(Password)
Jane	0x23da09bf
Patrick	0x89bbc234
Philip	0x320cfd9e
Roz	0x89bbc234
Claire	0x2dec9a10



Defense: Hashed Passwords

Identity	h(Password)
Jane	0x23da09bf
Patrick	0x89bbc234
Philip	0x320cfd9e
Roz	0x89bbc234
Claire	0x2dec9a10



Pre-computed Dictionary Attack



Password	h>Password)
qwerty	0x89bbc234
12345678	0xcafe8900
password	0x424523d3
11111111	0xde334211
p2ssw0rd!	0x23da09bf



Identity	h>Password)
Jane	0x23da09bf
Patrick	0x89bbc234
Philip	0x320cfd9e
Roz	0x89bbc234
Claire	0x2dec9a10

Pre-computed Dictionary Attack



Password	h>Password)
qwerty	0x89bbc234
12345678	0xcafe8900
password	0x424523d3
11111111	0xde334211
p2ssw0rd!	0x23da09bf

Identity	h>Password)
Jane	0x23da09bf
Patrick	0x89bbc234
Philip	0x320cfd9e
Roz	0x89bbc234
Claire	0x2dec9a10



Pre-computed Dictionary Attack



Password	h>Password)
qwerty	0x89bbc234
12345678	0xcafe8900
password	0x424523d3
11111111	0xde334211
p2ssw0rd!	0x23da09bf

Identity	h>Password)
Jane	0x23da09bf
Patrick	0x89bbc234
Philip	0x320cfd9e
Roz	0x89bbc234
Claire	0x2dec9a10



Defense: Iterated Hashing

d iterations

Identity	$h(h(h(\dots(\text{Password}))))$
Jane	0x356323da
Patrick	0x094f89bb
Philip	0x987cca21
Roz	0x094f89bb
Claire	0x23c29585



Defense: Salting

Identity	Salt	h>Password,Salt)
Jane	0xdef	0x93762d21
Patrick	0x32c	0x2874efa2
Philip	0xfef	0x954eabbc
Roz	0xcaf	0x5609ab1c
Claire	0x835	0xfe3dc550



Password Requirements....

Password Requirements

- Chosen uniformly at random
- Easy to remember