

10/2/26

COMP 435:

Computer Security Concepts



Lecture 18: Password Guessing!



The University
of North Carolina
at Chapel Hill

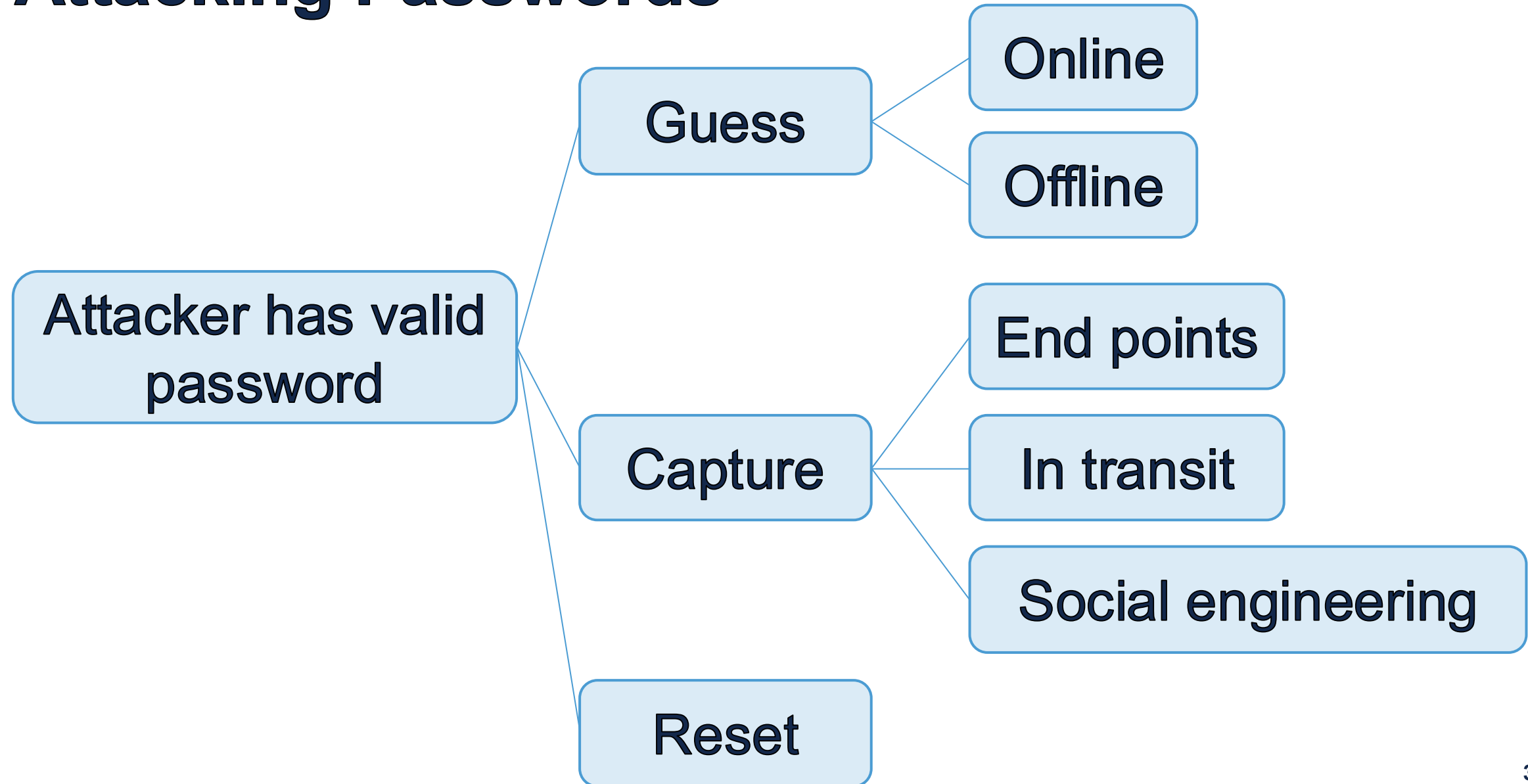
<https://tinyurl.com/comp435-fa26>

Logistics Update

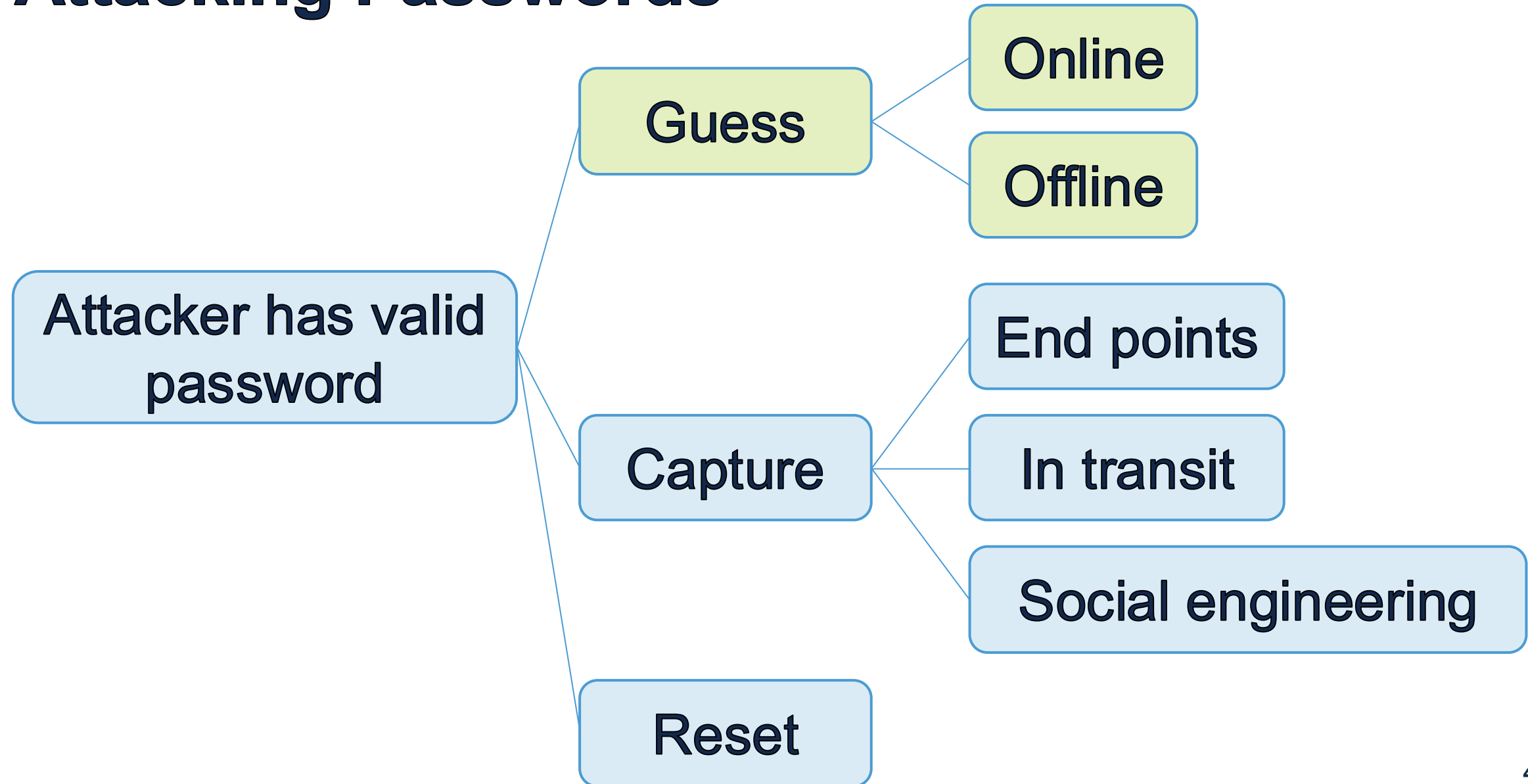


- Lab 2 Released! Due 10/14
- WA3 In-Class On Friday – 70% of Grade
 - In-Class component due tomorrow night! 30% Should take 20 mins
 - Password guessing activity! 😊
- All in-class Friday WA days posted on assignments tab

Attacking Passwords



Attacking Passwords





Online Guessing Attacks

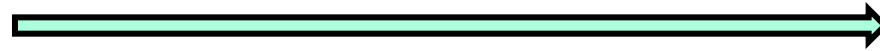
Attacker



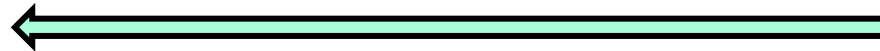
Resource



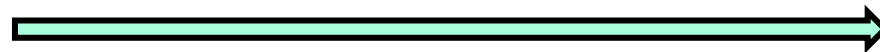
alice, 1234



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\$oTo!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

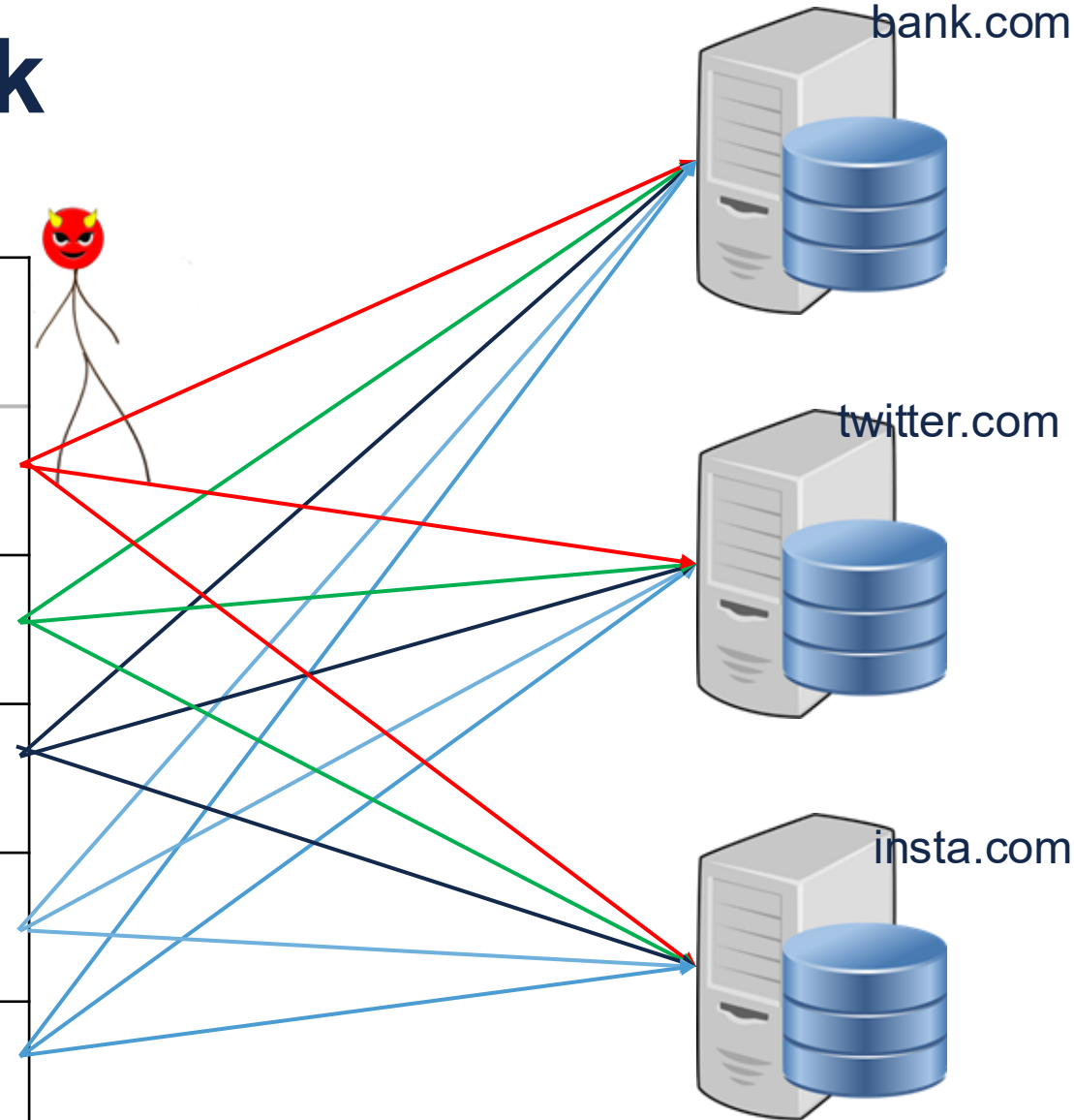
*try “querty” until
we get a hit!*

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\$oTo!4



Defense: Hashed Passwords



A **hashed value** is a fixed-length string produced by applying a **hash function** to input data.

Easy to compute, but **hard to reverse**.

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

Defense: Hashed Passwords

A **hashed value** is a fixed-length string produced by applying a **hash function** to input data.

Easy to compute, but **hard to reverse**.

Weakness: Hash algorithms are deterministic → same inputs produces the same output.



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



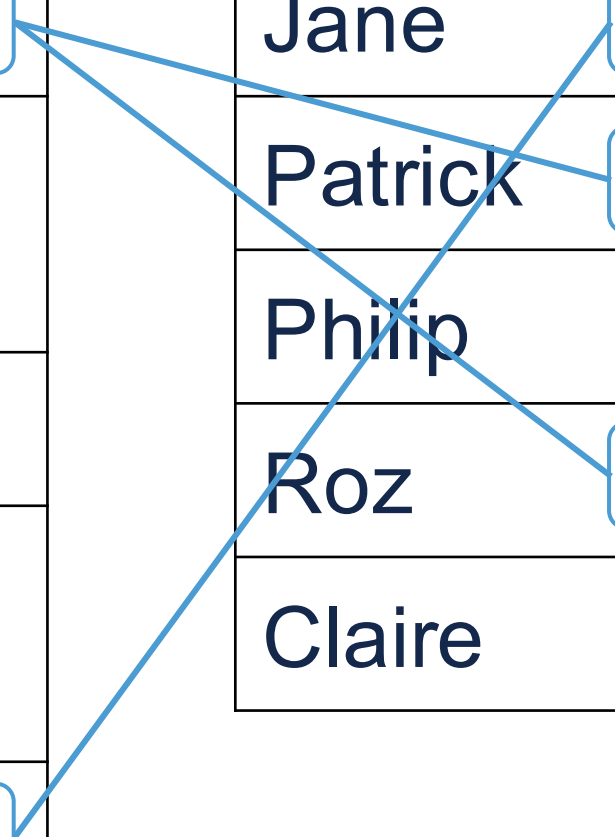
Pre-computed Dictionary Attack



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



Server computes the hash of the hash of the password.

Goal: makes building the pre-computed hash prohibitively expensive.

d iterations

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

Defense: Salting



Salt: a string unique to that user

Concatenate it to the password
before hashing!

We are **not adding a secret**.
Just making it harder to reverse engineer

Now, the attacker has to compute
the hash value of all possible salt
values concatenated with all likely
passwords

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

Plan for Class Today



- 10:10-10:25 – Password Background
 - 10:35-11:00 – Password guessing activity!
-

Guiding Question 😊

How do we choose good passwords?