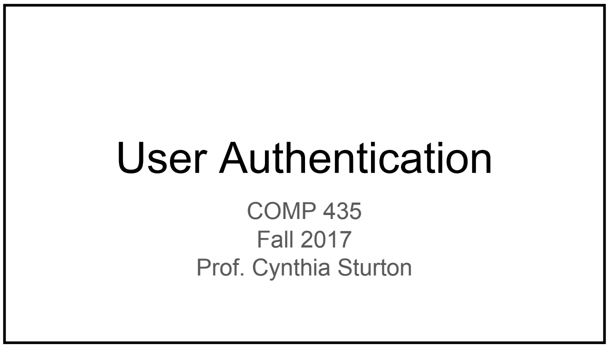
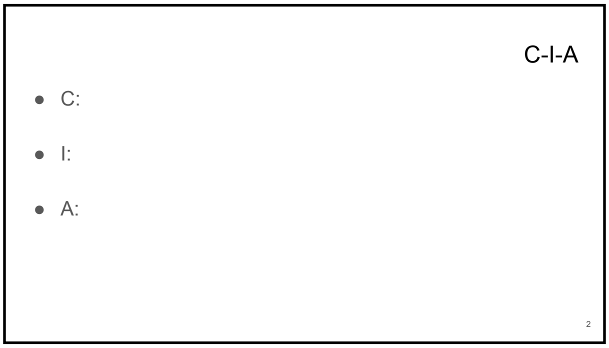


User Authentication

COMP 435
Fall 2017
Prof. Cynthia Sturton

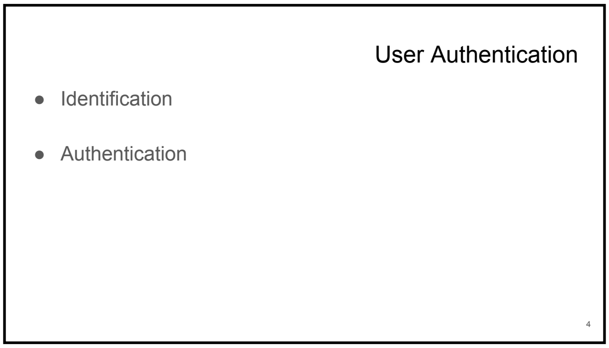


C-I-A

- C:
- I:
- A:

C-I-A

- C: only **authorized users** can read
- I: only **authorized users** can modify
- A: all **authorized users** have access



User Authentication

- Identification
- Authentication

Identification

- Explicit:

  “Hello, my name is”
- Implicit:

  Wearing an orange apron at Home Depot

Identification & Authentication

- ID: state your name when you ask a question
  Auth: none

- ID: your presence in the classroom
  Auth: attendance sheet sign-in

Identification vs. Authentication

Identification

- Public

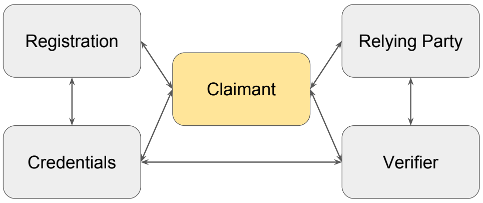
- Well-known

Authentication

- Private

- Something you know
- Something you have
- Something you are
- Something you do

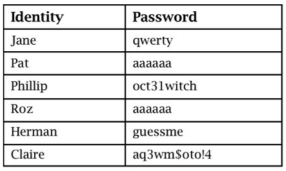
Identification & Authentication



Passwords: something you know

- Ubiquitous
- Difficult to use well
- Easy to attack

Password-based Authentication



Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Attacking Password-based Authentication

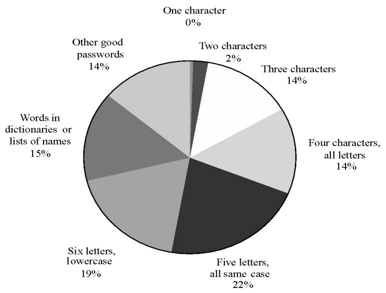
- Guessing
- Workstation hijacking
- Social engineering
- Electronic monitoring

Character Sets used in Password	Calculation	Possible Combinations
Dictionary words	---	600,000
Numbers only	10^8	100,000,000
Lowercase alpha	26^8	208,827,064,576
Full alpha	52^8	53,459,728,531,456
Full alpha + number	62^8	218,340,105,584,896
Printable characters	(10+26+26+19)^8	645,753,531,245,761

https://www.uc.edu/infosec/password/choosepassword.html

Password-based Authentication

Passwords are unique and chosen uniformly and at random from the set of all possible passwords

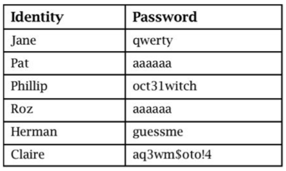


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Common Passwords

- “Qwerty”
- “Password”
- “123456”
- User’s family names
- Words in the dictionary
- Common number substitutions (3-e, 1-l, 4-for, 0-O)

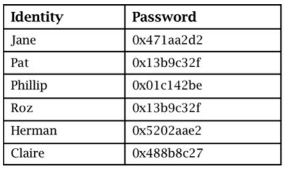
Attacking Passwords: guessing



Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Password-based Authentication



Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

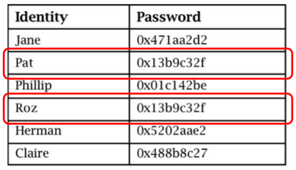
Hashed

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Offline Dictionary Attack

Precomputed list of popular passwords

Passwords



Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Hashed

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Salting the Passwords

Identity	ID+password	Stored authentication value
Jane	Jane+qwerty	0x1d46e346
Pat	Pat+aaaaaaa	0x2d5d3e44
Phillip	Phi+oct31witch	0xc23c04d8
Roz	Roz+aaaaaaa	0xe30f4d27
Herman	Her+guessme	0x8127f48d
Claire	Cla+aq3wm$oto!r	0x52093942

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Rainbow Table

Precomputed list of popular passwords, salted and hashed

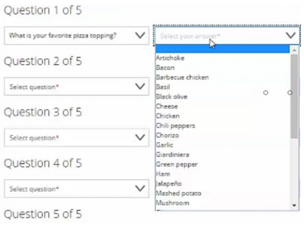
Strong Passwords

- Chosen uniformly and at random from the set of possible passwords
- Easy to remember

Q&A: something you know

- Register by answering a few questions about yourself
- Design assumptions:
  - Easier to remember
  - Adds entropy

United Airlines Using Q&A



Question 1 of 5

What is your favorite pizza topping?

Select your answer*

Artichoke
Bacon
Barbecue chicken
Basil
Black olive
Cheese
Chicken
Chili peppers
Chorizo
Garlic
Giardiniera
Green pepper
Ham
Jalapeño
Mashed potato
Mushroom

Question 2 of 5

Select question*

Question 3 of 5

Select question*

Question 4 of 5

Select question*

Question 5 of 5

http://krebsonsecurity.com/2016/08/united-airlines-sets-minimum-bar-on-security/