

2550 Intro to cybersecurity L3

abhi shelat

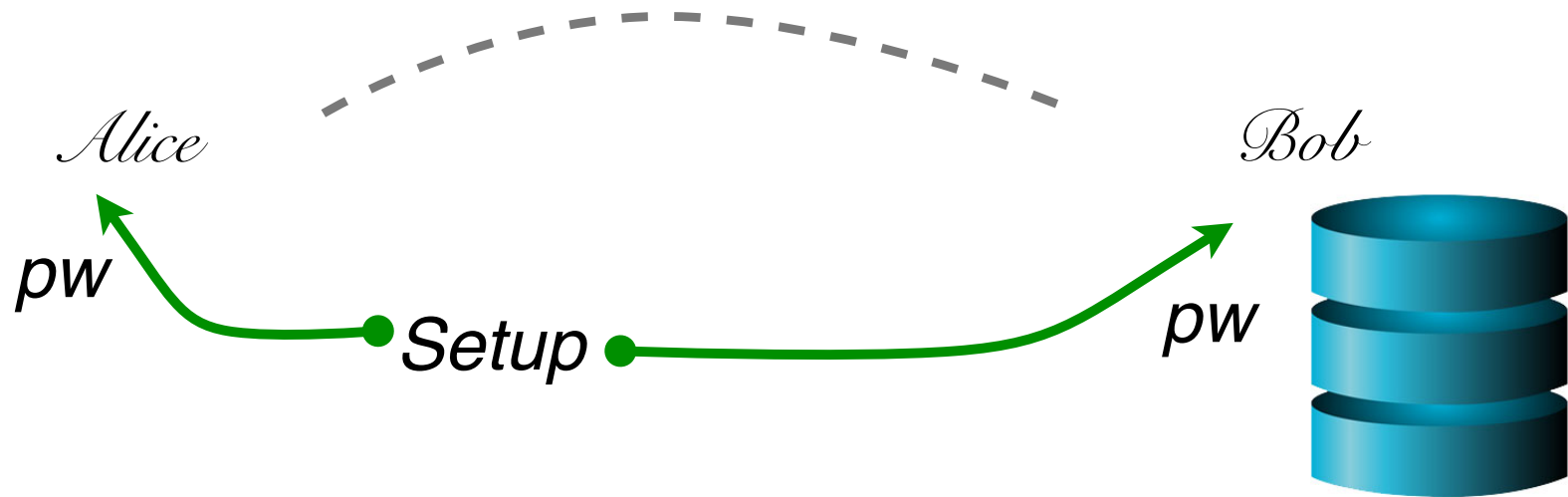
What are the steps of a password system?

setup, verification

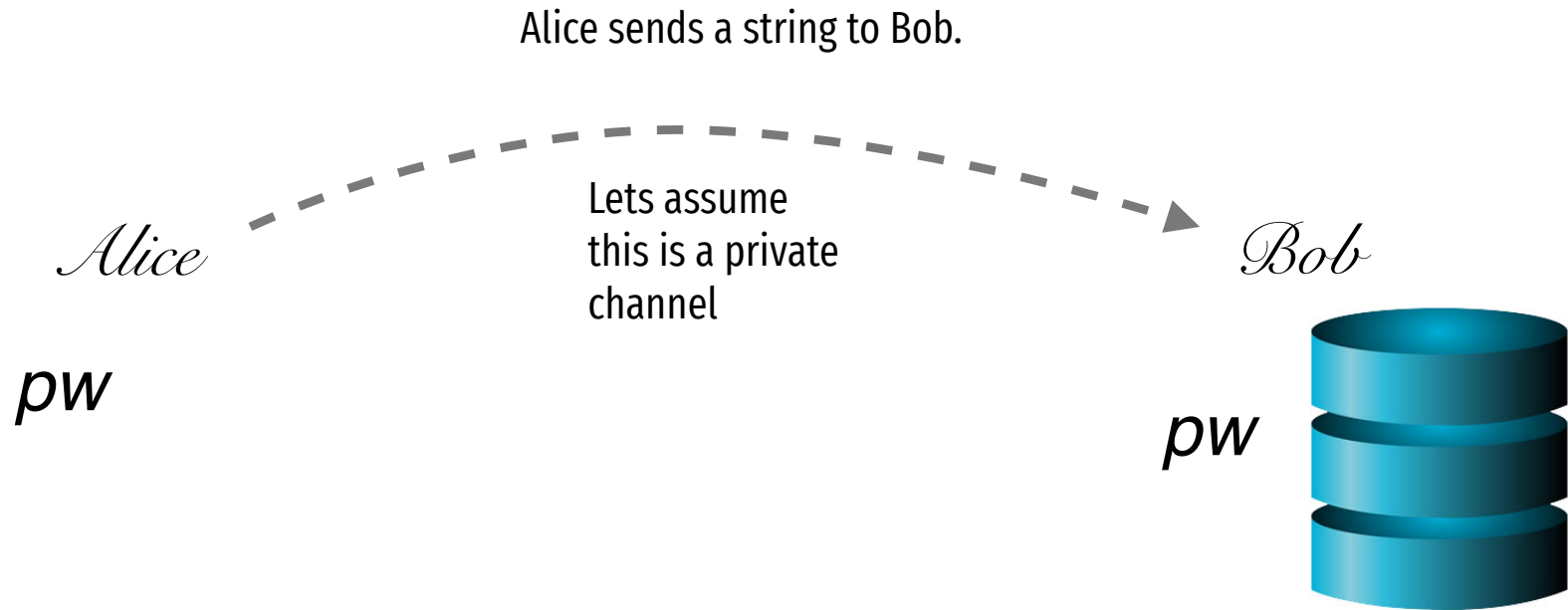
What properties do you expect?

Alice succeeds, Mallory fails

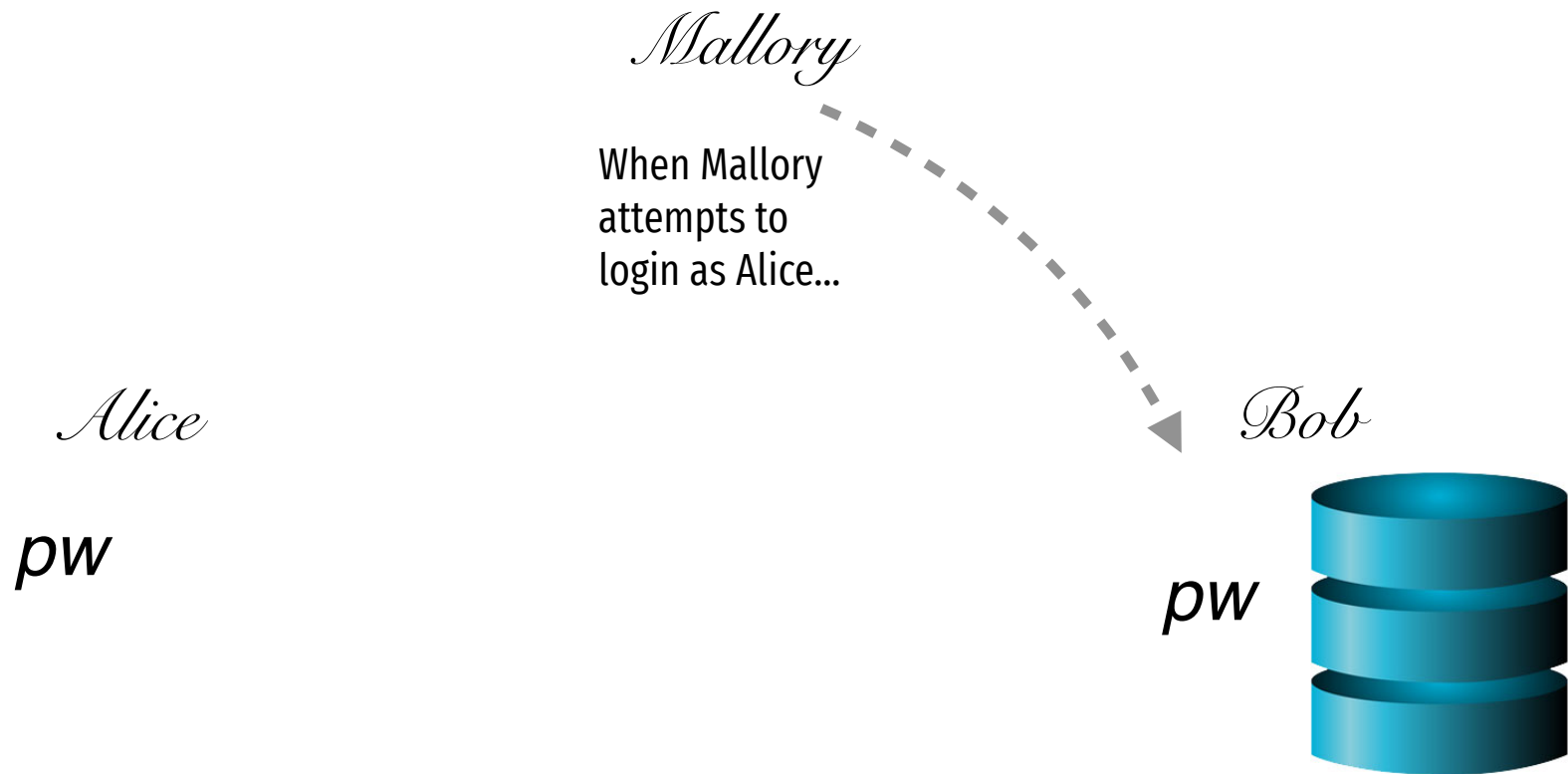
Passwords



Passwords: Alice always succeeds



Passwords: Others do not succeed



Failure of Operation

Failure of Abstraction

Recap

First systems: save the plaintext password in a file

Then they: hash the password and store hash.
to compare, hash the input and check equality.

But that also failed because:
use salting, add a random string to the
password and then hash. store the
random string next to the password.

4 upper/lower chars

2 digits

1 special char

jUsT33!

Recap

So third idea is to:

Failure of Operation

Humans pick easy-to-guess passwords.

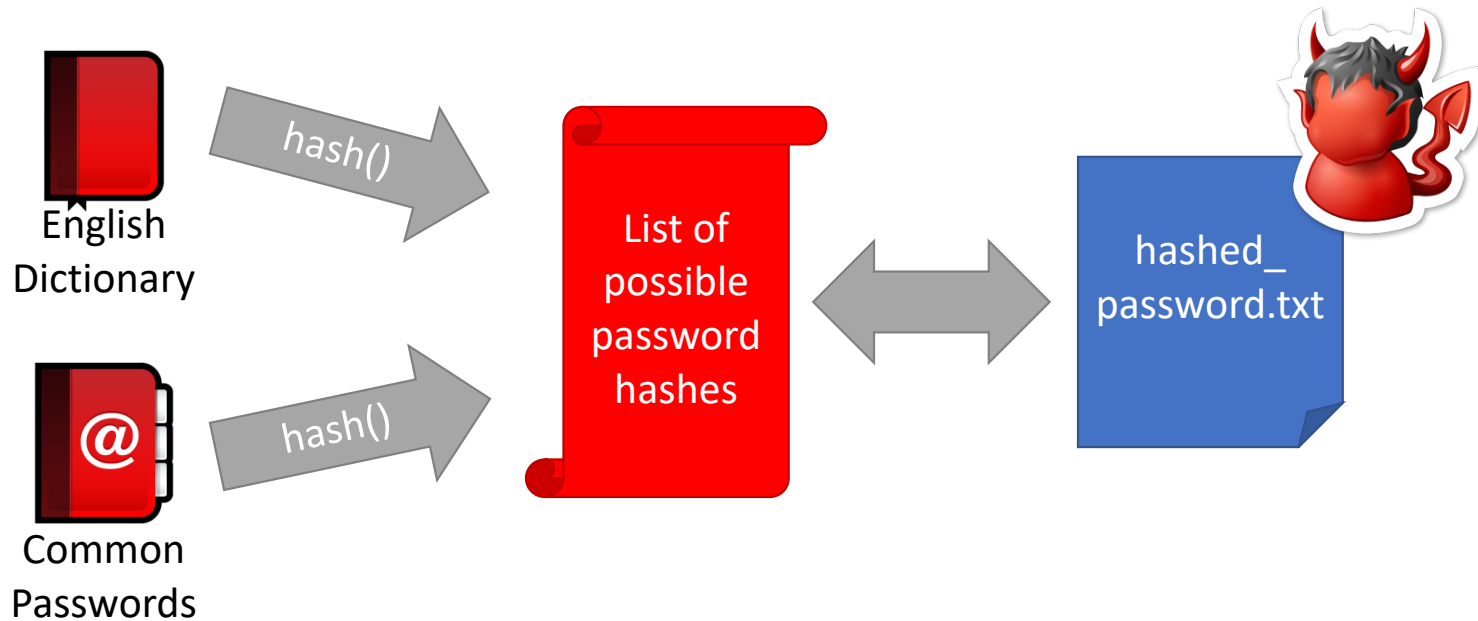
Failure of Abstraction

Humans are not capable of remembering hard-to-guess passwords.

Most Common Passwords

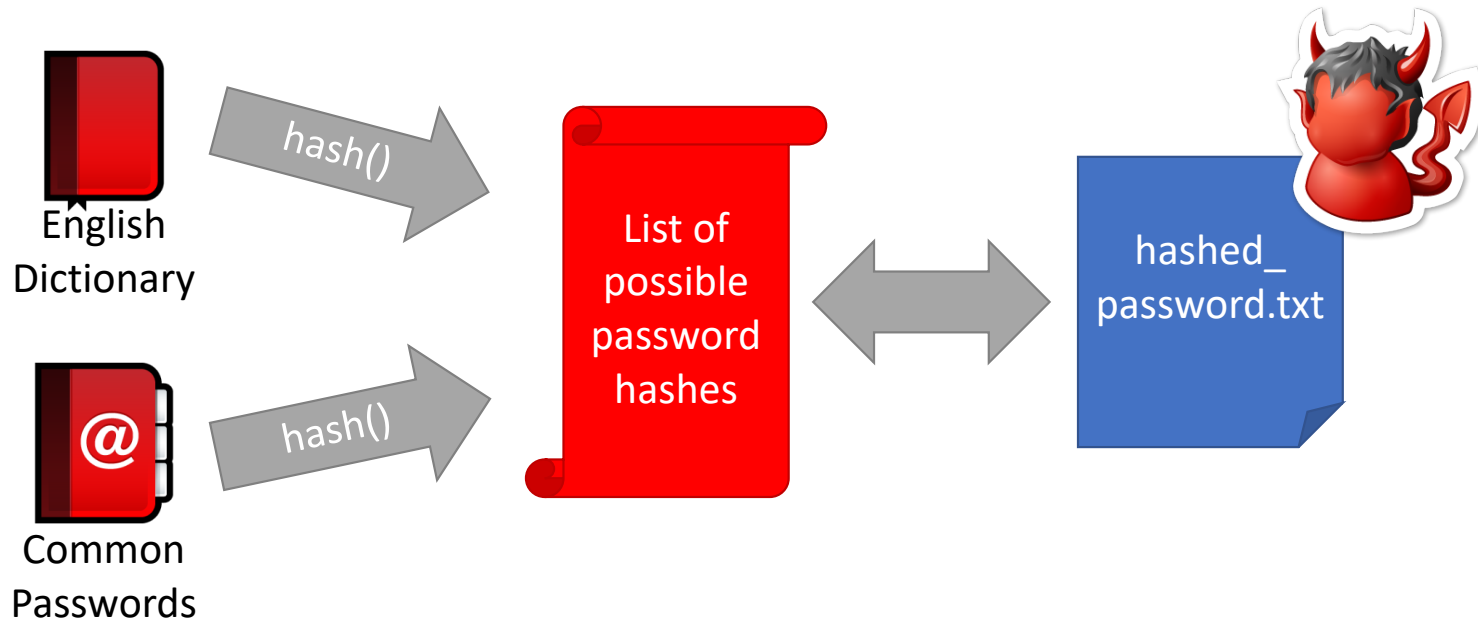
Rank	2013	2014
1	123456	123456
2	password	password
3	12345678	12345
4	qwerty	12345678
5	abc123	qwerty
6	123456789	123456789
7	111111	1234
8	1234567	baseball
9	iloveyou	dragon
10	adobe123	football

Dictionary Attacks



- Common for 60-70% of hashed passwords to be cracked in <24 hours

Dictionary Attacks



- Common for 60-70% of hashed passwords to be cracked in <24 hours

Brute force attack estimates

How big is the alphabet from which pwd are chosen?

Brute force attack estimates

How big is the alphabet from which pwd are chosen?

95 symbols

How long is a password?

Size of password domain:

Brute force attack estimates

Size of password domain: 95^8 6,634,204,312,890,625

<https://diskprices.com/?locale=us&condition=new>

Price per TB	Price	Capacity	Warranty	Form Factor	Technology	Condition	Affiliate Link
\$8.124	\$130	16 TB	5 years	Internal	SAS	New	MDD 16TB 7200RPM 256MB Cache SAS 12.0Gb/s 3.5inch Internal Enterprise Hard Drive (MDD16TSAS25672E) - [NOT a SATA HDD]
\$9.166	\$110	12 TB	3 years	Internal 3.5"	HDD	New	MDD 12TB 7200RPM SATA 6Gb/s 256MB Cache 3.5inch Internal Desktop Hard Drive, MD12TBGSA25672, Mechanical Hard Disk
\$10.00	\$100	10 TB	3 months	Internal	SAS	New	HUH721010AL4200 HGST Ultrastar He10 10TB 7200RPM SAS 12Gbps 256MB 2018
\$10.48	\$84	8 TB	3 years	Internal 3.5"	HDD	New	MaxDigitalData 8TB 7200 RPM 256MB Cache SATA 6.0Gb/s 3.5inch Internal Hard Drive for Surveillance (MD8000GSA25672DVR)
\$10.75	\$129	12 TB	3 years	Internal 3.5"	HDD	New	Seagate 12TB IronWolf NAS SATA Hard Drive 6Gb/s 256MB Cache 3.5-Inch Internal Hard Drive for NAS Servers, Personal Cloud Storage (ST12000VN0007)
\$10.81	\$86	8 TB	3 years	Internal 3.5"	HDD	New	MaxDigitalData 8TB 7200 RPM 256MB Cache SATA 6.0Gb/s 3.5inch Internal Hard Drive for NAS Network Storage (MD8000GSA25672NAS)
\$11.25	\$90	8 TB	3 years	Internal 3.5"	HDD	New	MaxDigitalData 8TB 7200 RPM 256MB Cache SATA 6.0Gb/s 3.5inch Internal Enterprise Hard Drive (MD8000GSA25672E) - 3 Years Warranty
\$11.87	\$190	16 TB		Internal 3.5"	HDD	New	16TB Exos X16 SATA 6Gb/s 7200RPM 3.5" Enterprise HDD — ST16000NM001G
\$13.33	\$80	6 TB	3 years	Internal 3.5"	HDD	New	MDD (MDD6TSATA6472DVR) 6TB 7200RPM 64MB Cache SATA 6.0Gb/s 3.5inch Internal Surveillance Hard Drive - 3 Years Warranty
\$13.33	\$40	3 TB		Internal	SAS	New	Seagate ST33000650SS Constellation ES.2 SAS 6Gb/s 3-TB Hard Drive

Attack 2: brute force attack

Mallory

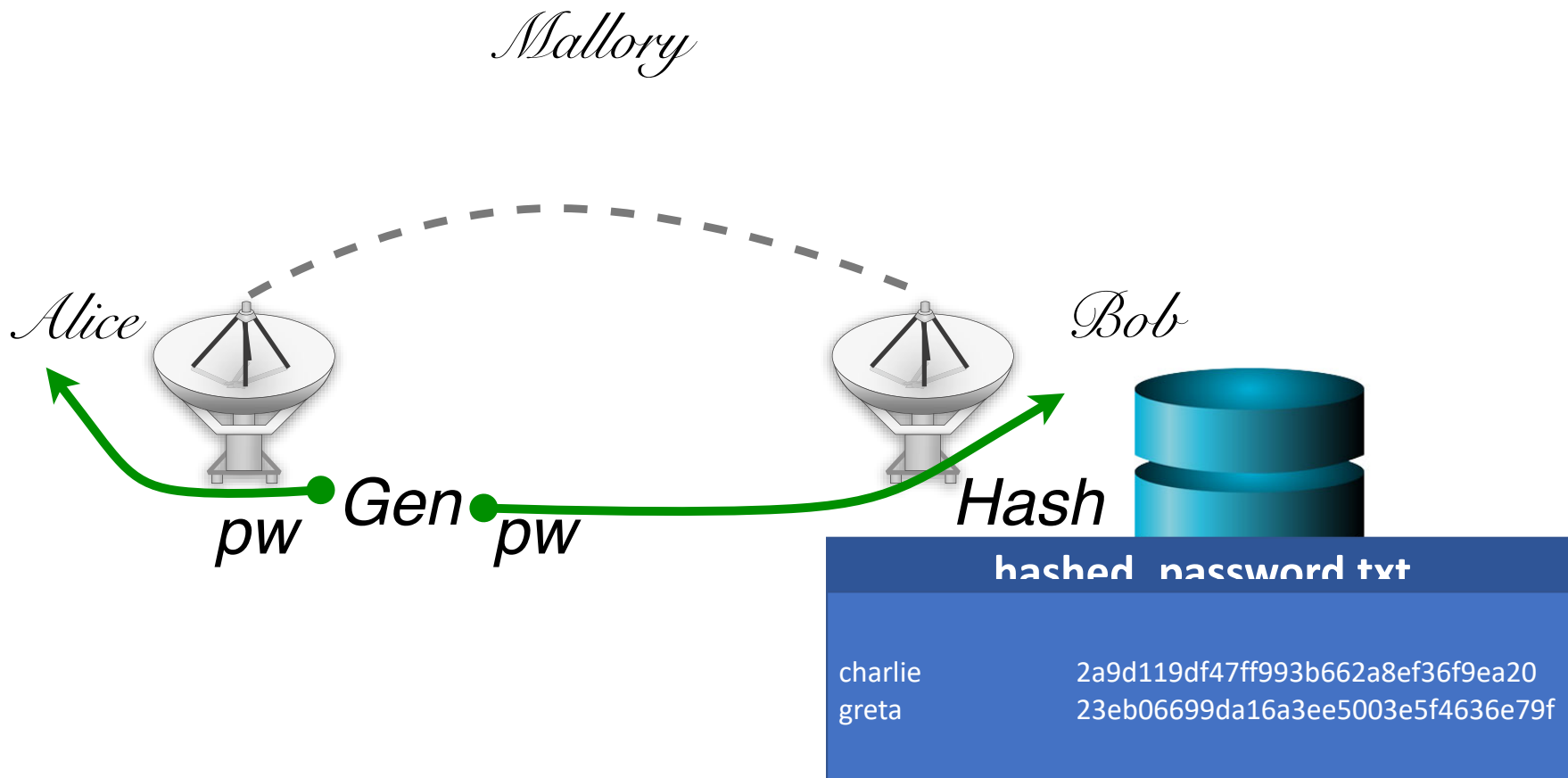
1. Buy storage system

- 2.

Bob



Attack 2: offline brute force



How to hamper offline brute force attacks?

Mallory

hashed password.txt	
charlie	2a9d119df47ff993b662a8ef36f9ea20
greta	23eb06699da16a3ee5003e5f4636e79f

Hardening Password Hashes

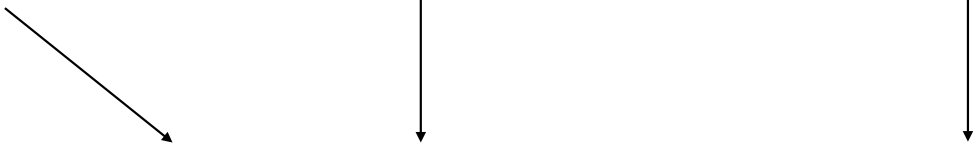
- **Key problem: cryptographic hashes are deterministic**
 - $\text{hash}(\text{'p4ssw0rd'}) = \text{hash}(\text{'p4ssw0rd'})$
 - This enables attackers to build lists of hashes
- **Solution: make each password hash unique**
 - Add a random **salt** to each password before hashing
 - $\text{hash}(\text{salt} + \text{password}) = \text{password hash}$
 - Each user has a unique, random salt
 - Salts can be stores in plain text

Example Salted Hashes

MD5 algorithm

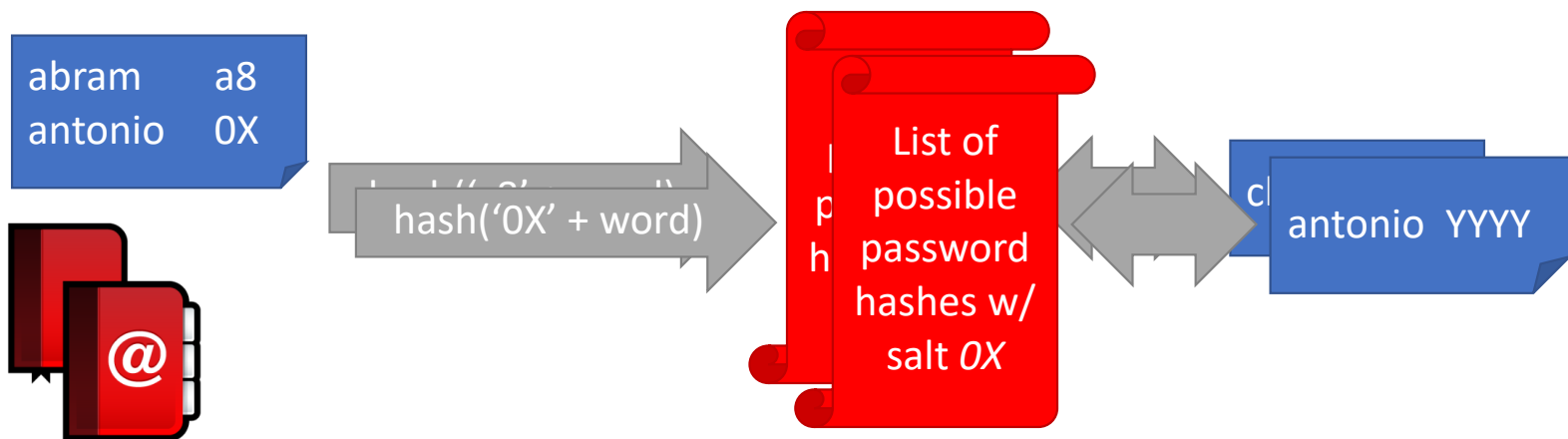
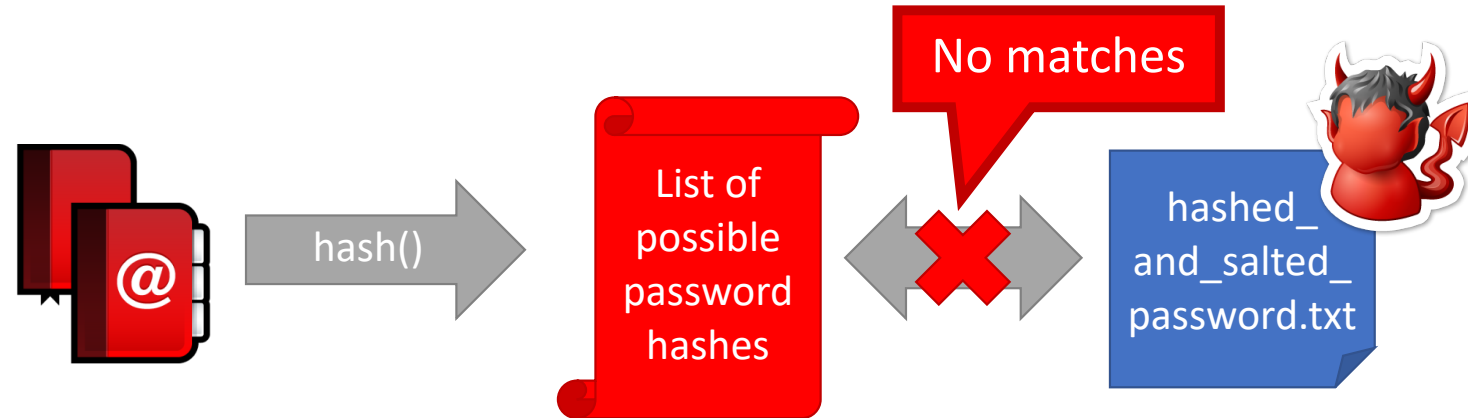
salt

hash



benvolio:\$1\$wSxbG4qj\$bm4SWOr5EG8KwxoIztctF0
abram:\$1\$oVoN6gZ1\$wZd8lNY0A7DGk7tSGhu3I/
antonio:\$1\$/nh0l9vD\$m04b0AIpaVjN0rvypUg9f.

Attacking Salted Passwords



Breaking Hashed Passwords

- **Stored passwords should always be salted**
 - Forces the attacker to brute-force each password individually
- **Problem: it is now possible to compute hashes very quickly**
 - GPU computing: hundreds of small CPU cores
 - nVidia GeForce GTX Titan Z: 5,760 cores
 - GPUs can be rented from the cloud very cheaply
 - \$0.9 per hour (2018 prices)

Examples of Hashing Speed

- A modern x86 server can hash all possible 6 character long passwords in 3.5 hours
 - Upper and lowercase letters, numbers, symbols
 - $(26+26+10+32)^6 = 690$ billion combinations
- A modern GPU can do the same thing in 16 minutes
- Most users use (slightly permuted) dictionary words, no symbols
 - Predictability makes cracking much faster
 - Lowercase + numbers $\rightarrow (26+10)^6 = 2B$ combinations

Hardening Salted Passwords

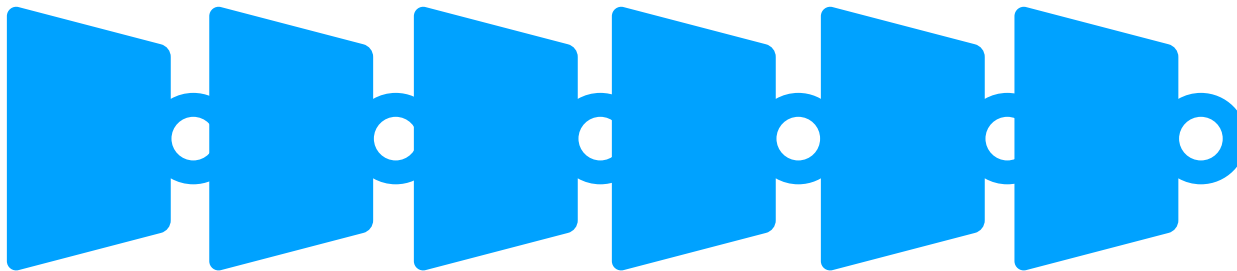
- Problem: typical hashing algorithms are too fast
 - Enables GPUs to brute-force passwords
- Old solution: hash the password multiple times
 - Known as [key stretching](#)
 - Example: *crypt* used 25 rounds of DES
- New solution: use hash functions that are designed to be **slow**
 - Examples: bcrypt, PBKDF2, scrypt
 - These algorithms include a [work factor](#) that increases the time complexity of the calculation
 - scrypt also requires a large amount of memory to compute, further complicating brute-force attacks

Slow hash movement



Iterated hash function {x times}

Pw
Salt

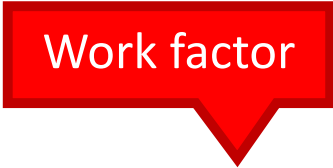


Hashed pwd

bcrypt Example

- Python example; install the *bcrypt* package

```
>>> import bcrypt
>>> bcrypt.hashpw(b'fooasdfsdf', bcrypt.gensalt(8))
```



Work factor

Best practices so far:

Dealing With Breaches

- Suppose you build an extremely secure password storage system
 - All passwords are salted and hashed by a high-work factor function
- It is still possible for a dedicated attacker to steal and crack passwords
 - Given enough time and money, anything is possible
 - E.g. The NSA
- Question: is there a principled way to detect password breaches?

Honeywords

- Key idea: store multiple salted/hashed passwords for each user
 - As usual, users create a single password and use it to login
 - User is unaware that additional **honeywords** are stored with their account
- Implement a **honeyserver** that stores the index of the correct password for each user
 - Honeyserver is logically and physically separate from the password database
 - Silently checks that users are logging in with true passwords, not honeywords
- What happens after a data breach?
 - Attacker dumps the user/password database...
 - But the attacker doesn't know which passwords are honeywords
 - Attacker cracks all passwords and uses them to login to accounts
 - If the attacker logs-in with a honeyword, the honeyserver raises an alert!

Honeywords example



Bob

SHA512("fl" | "p4ssW0rd") → bHDJ8l



Cracked Passwords

User	PW 1	PW 2	PW 3
Bob	123456	p4ssW0rd	Turtles!
sandi	puppies	iloveyou	blizzard
Alice	coff33	3spr3ss0	qwerty



Database



User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	pIDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5



Honeyserver



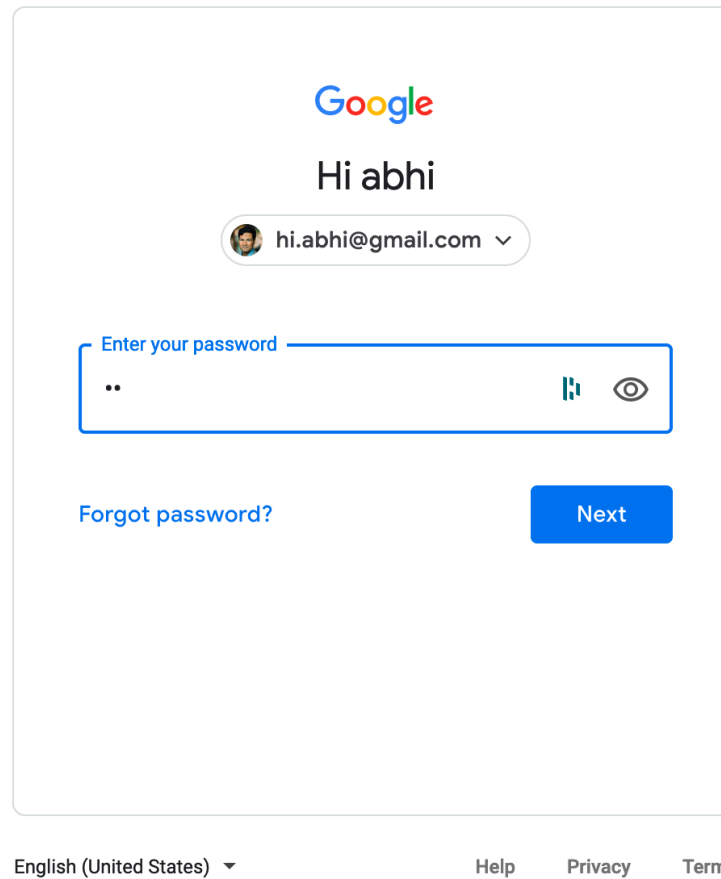
User	Index
Bob	2
sandi	3
Alice	1

Multiple layers of storage

Password Storage Summary

- 1. Never store passwords in plain text**
 - 2. Always salt and hash passwords before storing them**
 - 3. Use hash functions with a high work factor**
 - 4. Implement honeywords to detect breaches**
- These rules apply to any system that needs to authenticate users
 - Operating systems, websites, etc.

Still one problem?



The image shows a Google login interface. At the top is the Google logo. Below it, the text "Hi abhi" is displayed. Underneath is a dropdown menu showing a profile picture and the email address "hi.abhi@gmail.com" with a downward arrow. Below this is a password input field with the placeholder text "Enter your password". The field contains two dots, indicating a password is entered. To the right of the input field are icons for Google Assistant and a toggle for password visibility. Below the input field, there is a link "Forgot password?" and a blue "Next" button. At the bottom of the page, there is a language selector "English (United States)" with a dropdown arrow, and links for "Help", "Privacy", and "Terms".

Google

Hi abhi

hi.abhi@gmail.com ▼

Enter your password

..

[Forgot password?](#) [Next](#)

English (United States) ▼ [Help](#) [Privacy](#) [Terms](#)

Password Recovery/Reset

- Problem: hashed passwords cannot be recovered (hopefully)



“Hi... I forgot my password. Can you email me a copy? Kthxbye”

- This is why systems typically implement password **reset**
 - Use out-of-band info to authenticate the user
 - Overwrite `hash(old_pw)` with `hash(new_pw)`
- Be careful: its possible to crack password reset

Cracking Password Reset

- Typical implementations use Knowledge Based Authentication (KBA)
 - What was your mother's maiden name?
 - What was your prior street address?
 - Where did you go to elementary school
- Problems?
 - This information is widely available to anyone
 - Publicly accessible social network profiles
 - Background-check services like Spokeo
- Experts recommend that services not use KBA
 - When asked, users should generate random answers to these questions

Other roots of identity



Account recovery

 hi.abhi@gmail.com ▾

Enter the last password you remember using with this Google Account

Enter last password

[Try another way](#)

Next

English (United States) ▾

[Help](#)

[Privacy](#)

[Terms](#)

Forgot username or password

Identification

[Have a question? >](#)

Help us verify your identity.

For your security, please choose one of the options to verify your identity and provide the other requested information.

Choose one

Social Security number ▾

Social Security number

xxx-xx-xxxx 

Don't have a Social Security number? >

Account type

☒ Chase ATM/debit/prepaid card or credit card

☐ Chase commercial loan

☐ Other Chase account (e.g., checking, savings, mortgage application, commercial term loan, auto loan or lease)