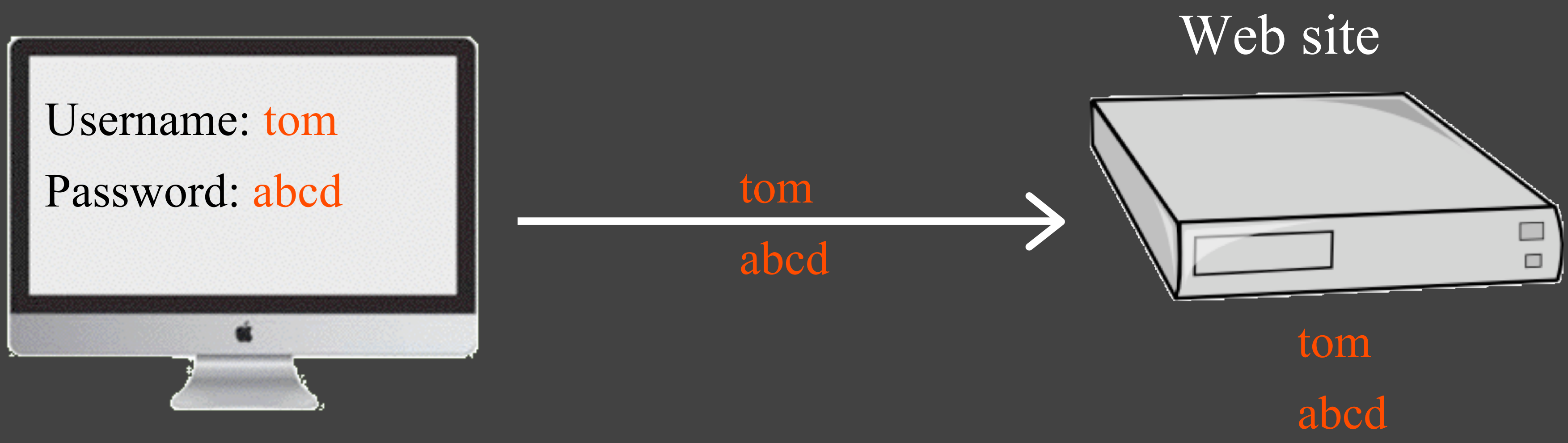
Tech Moment

Mashed Potatoes

By Tom Thorpe

- Familiar scenario

http Connection



Username: tom

Password: abcd

tom

abcd

Web site

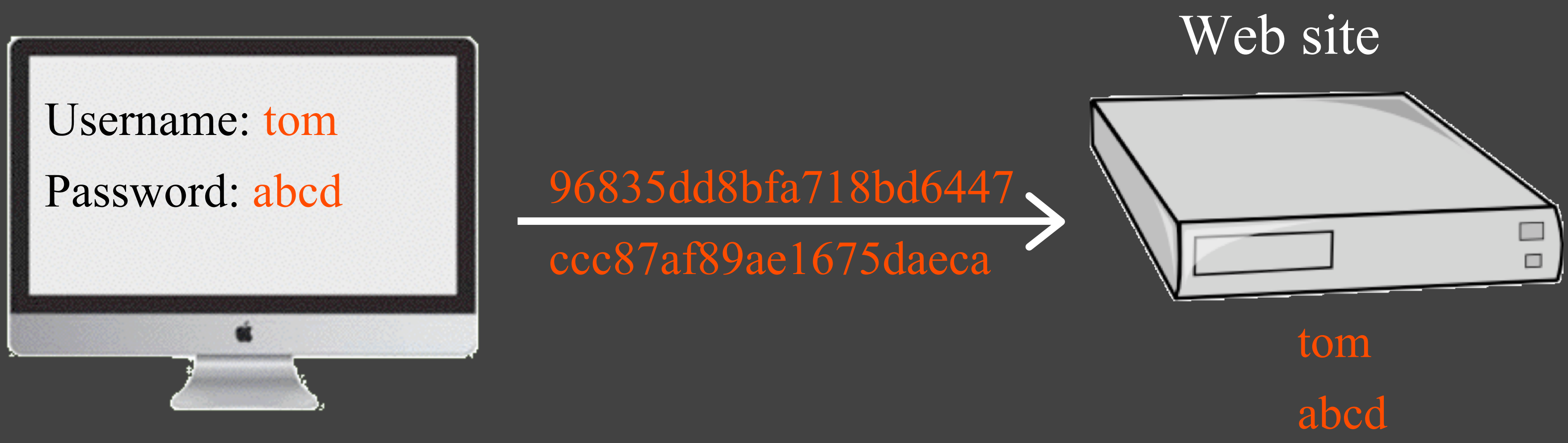
tom

abcd

Your password is SHOUTED down the internet.

NOT secure!

https Connection



Web site

Username: tom

Password: abcd

96835dd8bfa718bd6447

ccc87af89ae1675daeca

tom

abcd

Your password is whispered down the internet.

Secure from most prying eyes.

https Connection

- Secure Socket Layer / Transport Layer Security
- SSL/TLS is an encryption / decryption protocol developed for transmitting private data via the Internet
- SSL/TLS works by using a private key to encrypt and decrypt data that is transferred over the connection
- Most browsers support SSL/TLS
- Most sites which require sensitive information such as credit card information use SSL/TLS

What next?

- In both cases the site has your password
- If they are being hacked, the hacker has your user name password and, if you’ve used it more than once, can log into other sites as you
- Usually both are stored into a database

Therein lies another problem.
If the site gets hacked and
the database gets compromised.

Password Storage

- Method One: Plain text passwords

  How It Works: The simplest way a site can store your password. Your username and password are in a human-readable form.

  Does My Strong Password Matter? Not at all. If the site gets hacked, your password is easily accessible to anyone, no work required.

Password Storage [cont’d]

- Method Two: Basic password encryption

- How It Works: The site encrypts your password before they store it. Encryption uses a special key to turn your password into a random string of text. The key is often stored on the very same server that the passwords are on.

- Does My Strong Password Matter? No. Since it's easy to decrypt the password database with a key.

Password Storage [cont’d]

- Method Three: Hashed passwords

  How It Works: Hashed is similar to encryption in the sense that it turns your password into a long string of letters and numbers to keep it hidden. However, unlike encryption, hashing is a one way street: If you have the hash, you can't run the algorithm backwards to get the original password.

  Does My Strong Password Matter? Yes!

Password Storage [cont’d]

- Method Four: Hashed passwords with a dash of salt

  How It Works: Salting a hash means adding a random string of characters—called a "salt"—to the beginning or end of your password before hashing it. It uses a different salt for each password. Even if the salts are stored on the same servers, it will make it very hard to find those passwords since each one is long, complex, and unique.

  Does My Strong Password Matter? Yes!

Password Storage [cont'd]

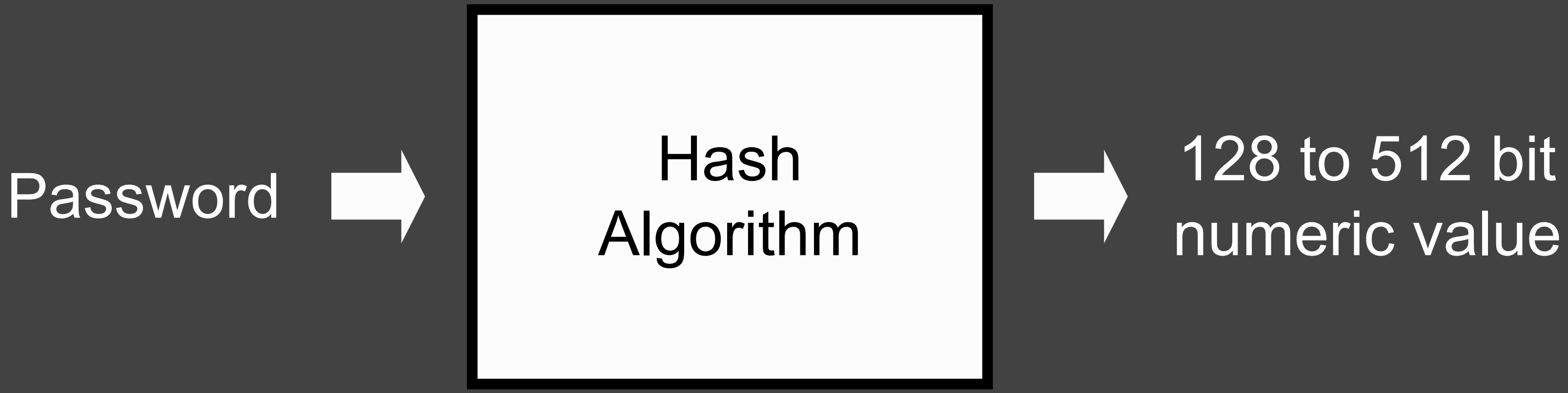
- Method Five: Slow hashes

  How It Works: Right now, most security experts are pointing to slower hashes as the best option for storing passwords. Classical hash functions are relatively fast. In a brute force attack, time is the most important factor. By using a slower hash brute force attacks take much, much longer.

  Does My Strong Password Matter? Since strong passwords are harder to brute force a strong password can definitely help you out here.

Hash Algorithms

- MD5
  - Designed by Ronald Rivest in 1991
  - Produces a 128-bit hash value
  - In 2004 serious flaws were discovered in MD5
- SHA-1
  - Designed by the United States National Security Agency
  - Produces a 160-bit hash value
  - Commonly used but on its way out now
- SHA-2
  - Consists of six hash functions
  - Produces 224-bit, 256-bit, 384-bit or 512-bit hash values



Password

Hash Algorithm

128 to 512 bit numeric value

Allison’s Analogy

Password Storage

Q. How do you know which method the web site uses?

A. You don’t!

But:

- If they can send you your password they are using methods 1 or 2. Beware!!!
- If all they can do is reset it (change it to one of their liking) then it is probably methods 3, 4, or 5

What Happens If a Web Site Is Hacked?

- The hacker gets the user/password database
- If the site stores passwords as hashes it might look like this:

```
  Username                    Password

imacelebrity   81fe8bfe87576c3ecb22426f8e57847382917acf
tt90210        96835dd8bfa718bd6447ccc87af89ae1675daeca
catlover       9d989e8d27dc9e0ec3389fc855f142c3d40f0c50
...
billygates     0a417f5c4d1afe0784b861dc32b23ab9aa329bcf
mgates         0a417f5c4d1afe0784b861dc32b23ab9aa329bcf
```

From Hash to Password

- Step 1 - Create a table of possible passwords and their hashes
- Step 2 - Compare the hash values in your table with the values in the stole database

Shortcut: Use any of the following attack software

Brutus
Cain and Abel
Crack
Aircrack-ng
John the Ripper
Airodump-ng
L0phtCrack
Metasploit Project
Ophcrack

Step 1) Create a table

- For simplicity, assume only lower case alphabetic characters
- Use SHA-1 hashes

Step 1) Create a table [cont'd]

- Start simple, 1 letter passwords

```
a               86f7e437faa5a7fce15d1ddcb9eaeaea377667b8
b               e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98
c               84a516841ba77a5b4648de2cd0dfcb30ea46dbb4
...
z               395df8f7c51f007019cb30201c49e884b46b92fa
```

- 26 entries

Step 1) Create a table [cont’d]

- 2 letter passwords

```
aa               e0c9035898dd52fc65c41454cec9c4d2611bfb37
ab               da23614e02469a0d7c7bd1bdab5c9c474b1904dc
ac               0c11d463c749db5838e2c0e489bf869d531e5403
...
zz               d7dacae2c968388960bf8970080a980ed5c5dcb7
```

- 26 x 26 = 676 entries

Step 1) Create a table [cont’d]

- 3 letter passwords

aaa	7e240de74fb1ed08fa08d38063f6a6a91462a815
aab	279117a46e6e3c76535b7899f9d58490a4755afc
aac	6d62bdf36d6d7705714d84161ea451d1a104d6cd
...	
zzz	ab5a81fe2f77397a478d89f41887867afcdca151

- 26 x 26 x 26 = 17,576 entries

Step 1) Create a table [cont’d]

- 4 letter passwords

```
aaaa           70c881d4a26984ddce795f6f71817c9cf4480e79
aaab           f1abd73aa0858634f18d36bf5666194958a8b7d2
aaac           00b25f15212ed225d3389b5f75369c82084b3a76
...
zzzz           cb990257247b592eaaed54b84b32d96b7904fd95
```

- 26 x 26 x 26 x 26 = 456,976 entries

Step 1) Create a table [cont’d]

- All English words

```
aardvark       ff49abca9701606b01b6245d587d26c31b63a433
aardwolf       661e46b960572398e02f82878e2dfeadb4518899
aaronic        7caef96c03644f58943f19e4182dd147df38ab7a
...
zythum         3ba044f0dcb1fd358423a56e0b21ec23bd73c55d
```

- Webster's Third New International Dictionary has some 470,000 entries

Step 1) Create a table [cont’d]

- Add 6,000 common first names
- Add 90,000 common last names

- Total of about a million so far

Real tables have a trillion entries

Step 2) Compare the hash values [cont'd]

- Stolen database

Username	Password
imacelebrity	81fe8bfe87576c3ecb22426f8e57847382917acf
catlover	9d989e8d27dc9e0ec3389fc855f142c3d40f0c50
...	

- Our table

...	
abcc	a788132b68ab69be57b4cfb76b661f001f41ed44
abcd	81fe8bfe87576c3ecb22426f8e57847382917acf
abce	0a431a7631cabf6b11b984a943127b5e0aa9d687
...	

Summary

- The site should always use https when sensitive information is involved
- Use good passwords, especially for sensitive sites
- Hope that those sites protect those passwords
- Change your password if the site gets hacked
- Never share a password between sites (unless you're OK with all the shared sites being able to log into each other as you)