CS 356 – Lecture 4
User Authentication

Spring 2024

Review

- Chapter 1: Basic Concepts and Terminology
  - Integrity, Confidentiality, Availability, Authentication, and Accountability
  - Types of threats: active vs. passive, insider/outsider
  - Lots of terminology and general concepts
- Chapter 2: Basic Cryptographic Tools
  - Symmetric key encryption and secure hashing
  - Public key cryptography
  - Random Numbers
- Chapter 3 – User Authentication

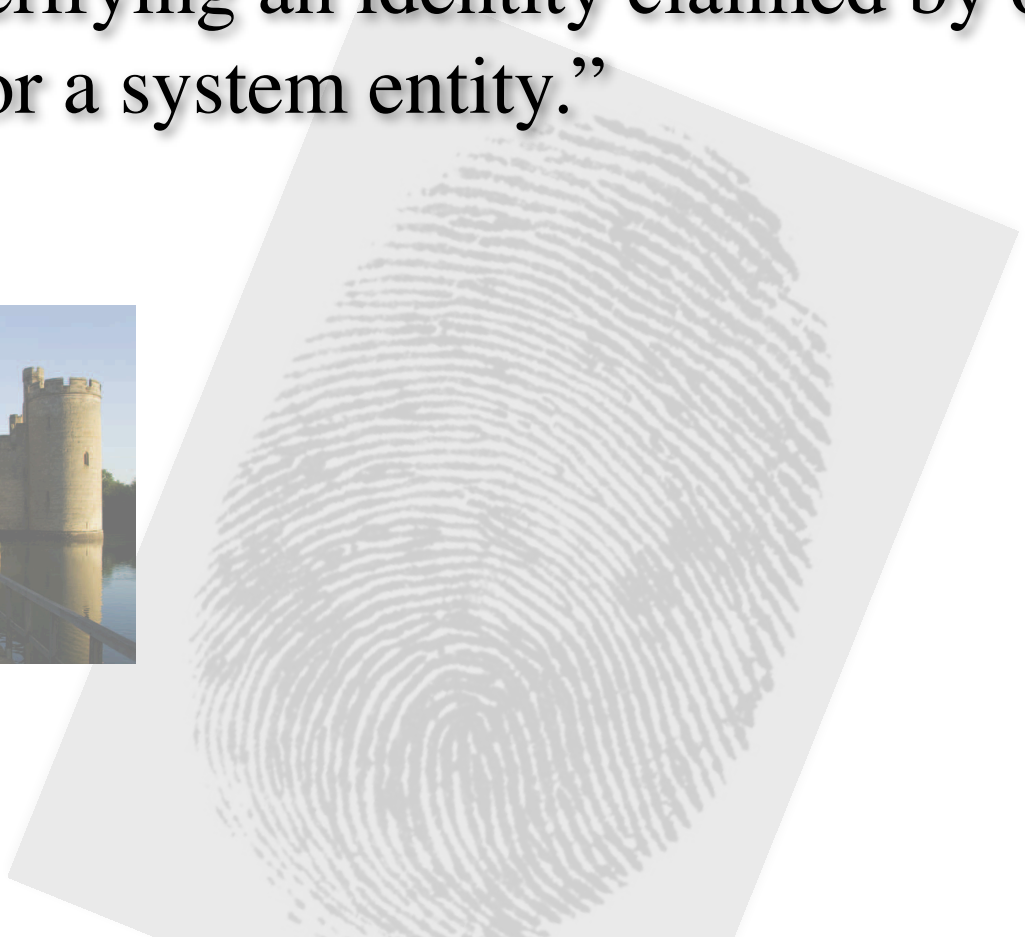
Chapter 3

User Authentication

RFC 2828

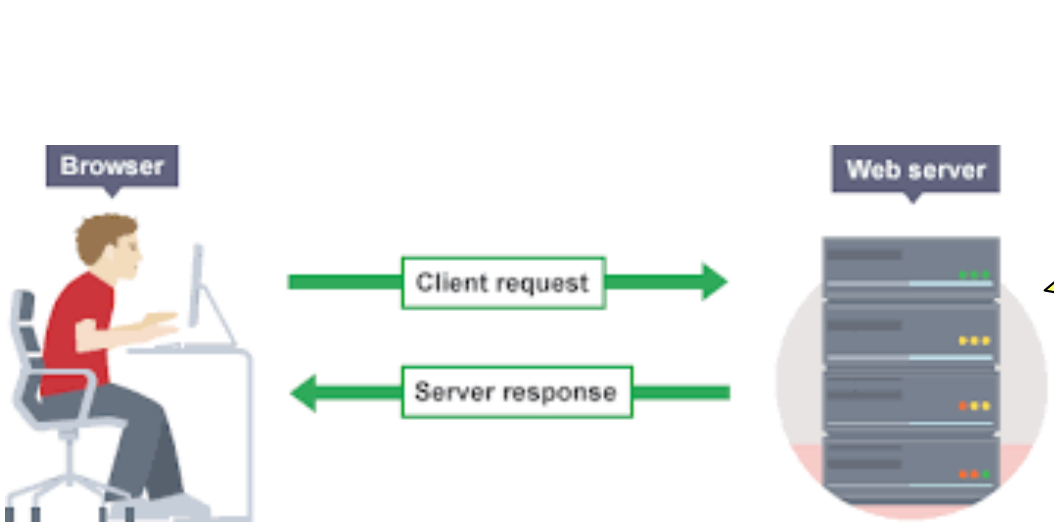
RFC 2828 defines user authentication as:

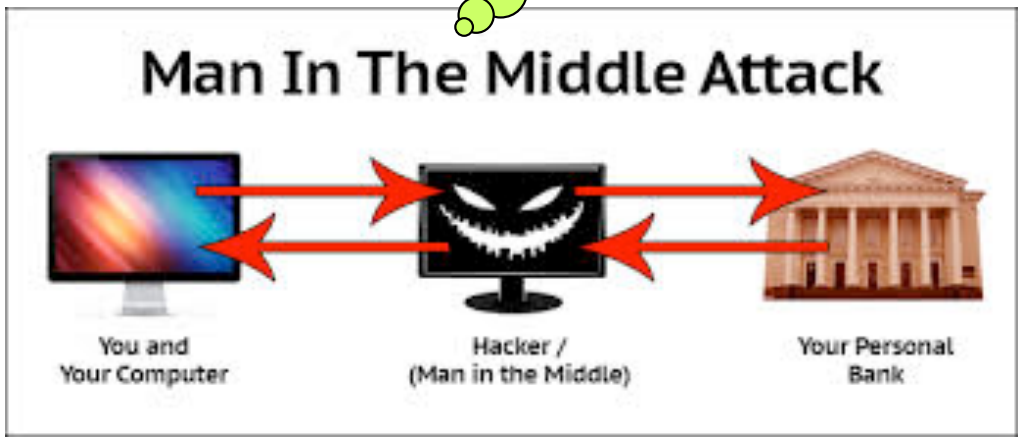
"The process of verifying an identity claimed by or for a system entity."



For Example...


FROM THE DIRECTOR OF HORRIBLE BOSSES
IDENTITY THIEF
SHE'S HAVING THE TIME OF HIS LIFE
FEBRUARY 8
THIS FILM IS NOT YET RATED
identitythiefmovie.com


Browser
Client request
Server response
Web server
I am your bank's webserver
No, I am your bank's webserver!


Man In The Middle Attack
You and Your Computer
Hacker / (Man in the Middle)
Your Personal Bank

"On the Internet, nobody knows you're a dog."

x

Authentication Process

- fundamental building block and primary line of defense
- basis for access control and user accountability

- identification step
  - presenting an identifier to the security system
- verification step
  - presenting or generating authentication information that corroborates the binding between the entity and the identifier

User Authentication

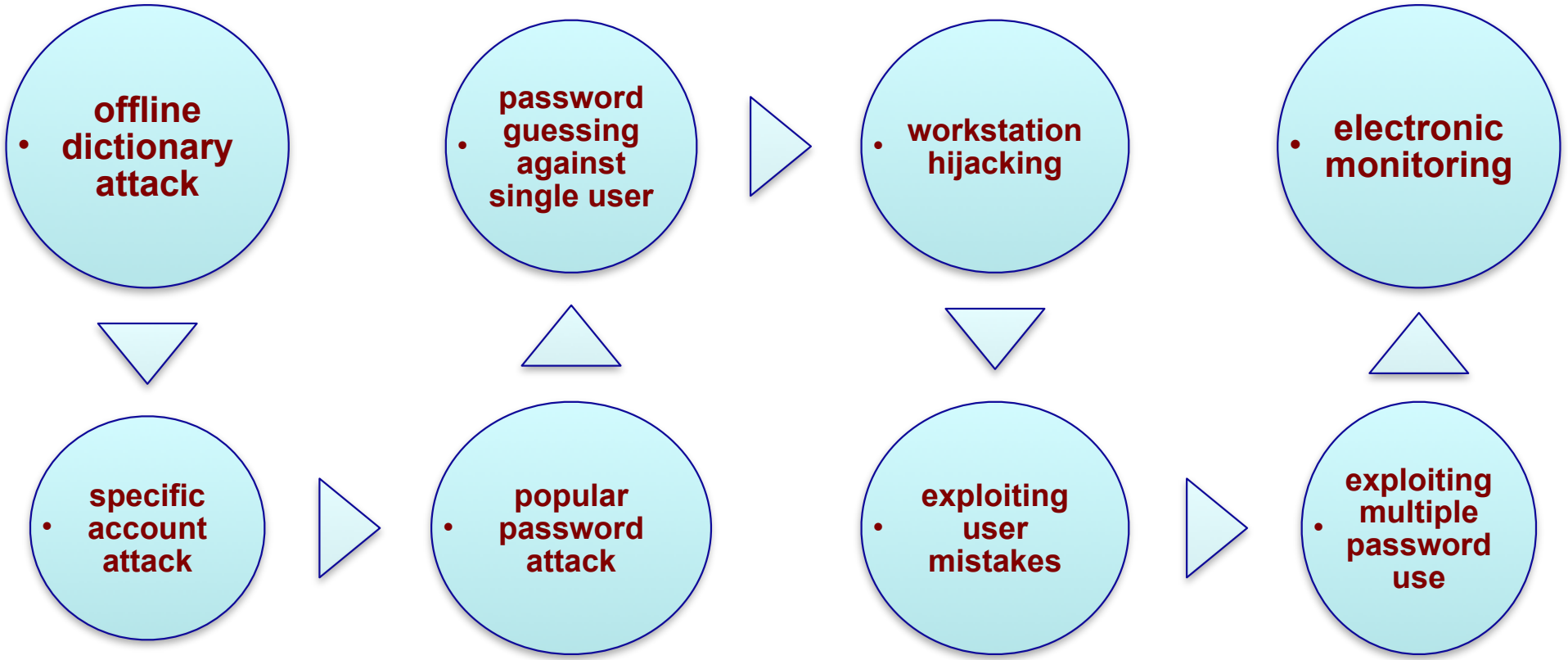
- **the four means of authenticating user identity are based on:**

something the individual knows	something the individual possesses (token)	something the individual is (static biometrics)	something the individual does (dynamic biometrics)
• password, PIN, answers to prearranged questions	• smartcard, electronic keycard, physical key	• fingerprint, retina, face	• voice pattern, handwriting, typing rhythm

Password Authentication

- widely used line of defense against intruders
  - user provides name/login and password
  - system compares password with the one stored for that specified login
- the user ID:
  - determines that the user is authorized to access the system
  - determines the user's privileges
  - is used in discretionary access control

Password Vulnerabilities



Countermeasures

- controls to prevent unauthorized access to password file
- intrusion detection measures
- rapid reissuance of compromised passwords
- account lockout mechanisms
- policies to inhibit users from selecting common passwords
- training in and enforcement of password policies
- automatic workstation logout
- policies against similar passwords on network devices

Use of Hashed Passwords

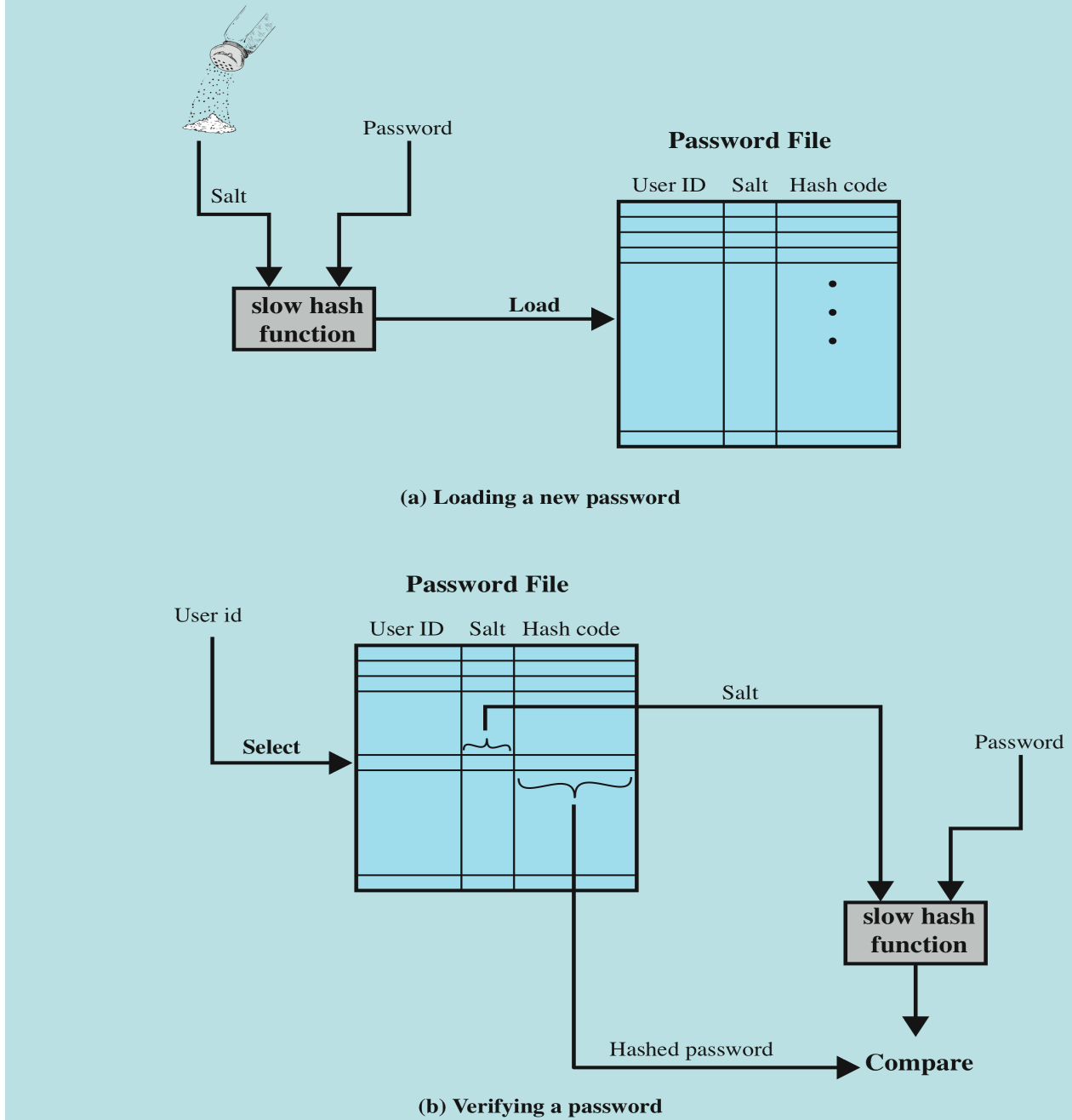
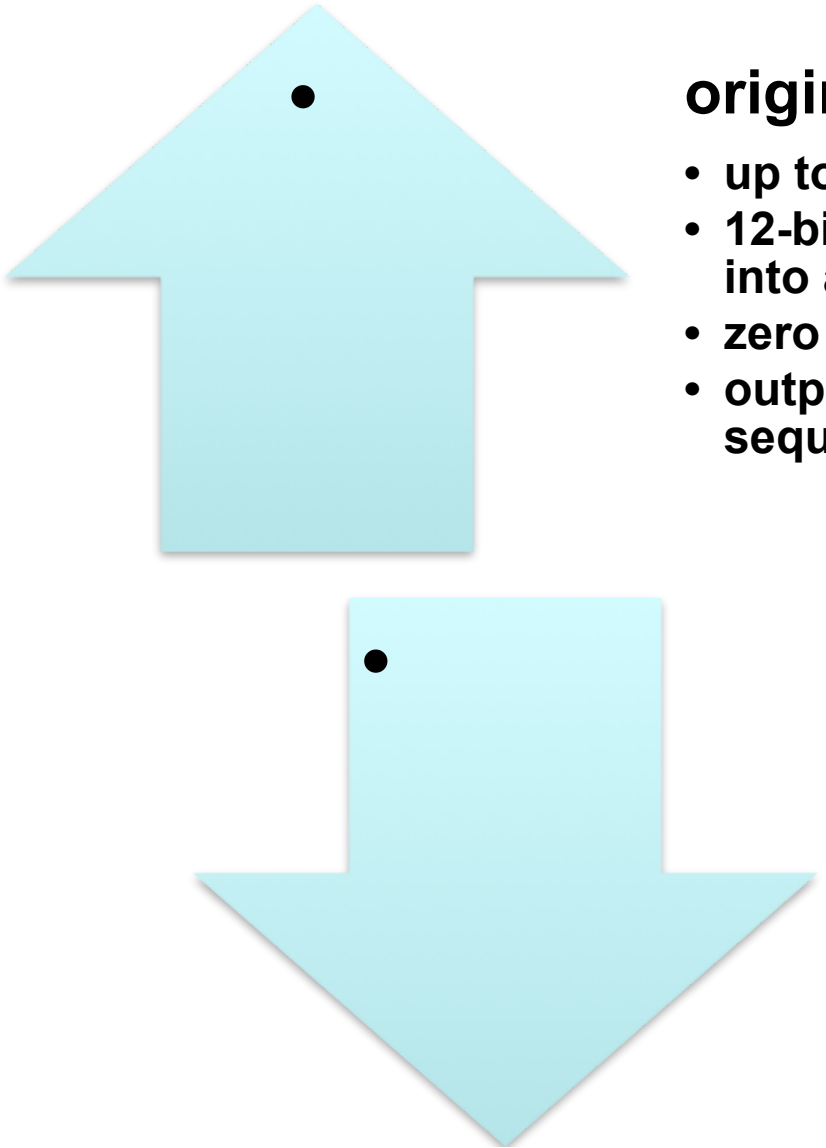


Figure 3.1 UNIX Password Scheme

UNIX Implementation



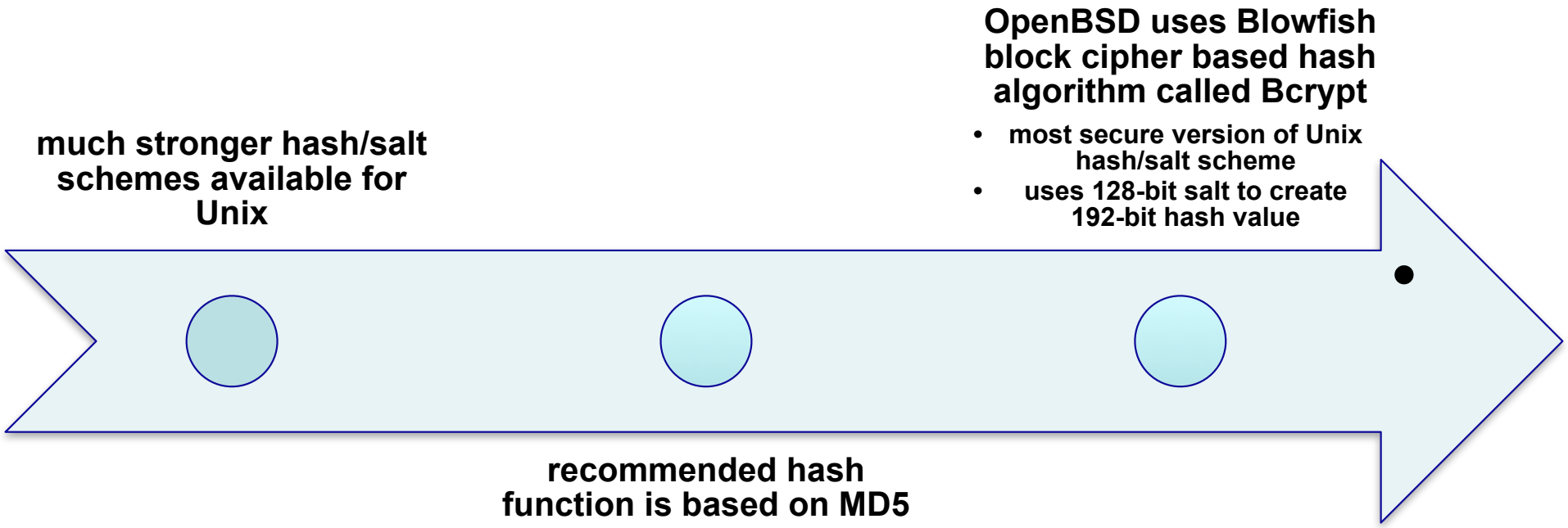
original scheme

- up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- zero value repeatedly encrypted 25 times
- output translated to 11 character sequence

now regarded as inadequate

- still often required for compatibility with existing account management software or multivendor environments

Improved Implementations

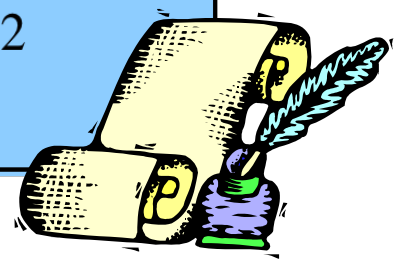


Password Cracking

- dictionary attacks
  - develop a large dictionary of possible passwords and try each against the password file
  - each password must be hashed using each salt value and then compared to stored hash values
- rainbow table attacks
  - pre-compute tables of hash values for all salts
  - a mammoth table of hash values
  - can be countered by using a sufficiently large salt value and a sufficiently large hash length

Observed Password Lengths

Length	Number	Fraction of Total
1	55	.004
2	87	.006
3	212	.02
4	449	.03
5	1260	.09
6	3035	.22
7	2917	.21
8	5772	.42
Total	13787	1.0



Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths and legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Passwords Cracked from a Sample Set of 13,797 Accounts

*Computed as the number of matches divided by the search size. The more words that need to be tested for a match, the lower the cost/benefit ratio.

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password[10]
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey
14	master	sunshine	letmein	abc123	111111	abc123	login
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars
17	bailey	welcome	monkey	access	master	flower	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd
20	123123	football	12345	michael	login	sunshine	master
21	654321	jesus	password1	superman	princess	master	hello
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx
25	Football	password1	000000	trustno1	starwars	password1	trustno1

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:

EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:

HARD

correct horse battery staple

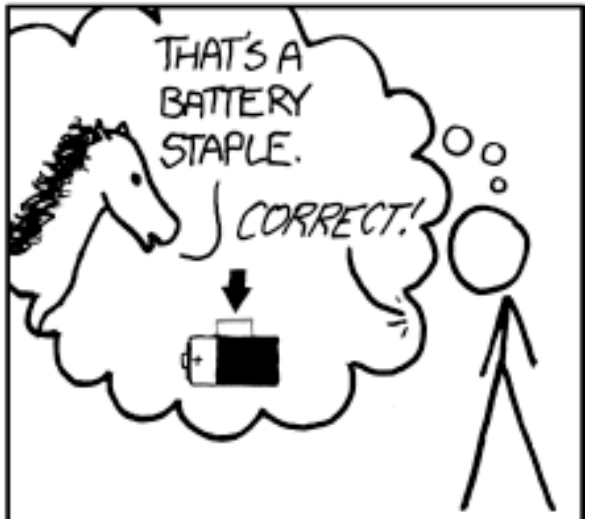
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:

HARD



DIFFICULTY TO REMEMBER:

YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password File Access Control

- can block offline guessing attacks by denying access to encrypted passwords

- make available only to privileged users

- shadow password file
  - a separate file from the user IDs where the hashed passwords are kept

- vulnerabilities
  - weakness in the OS that allows access to the file
  - accident with permissions making it readable
  - users with same password on other systems
  - access from backup media
  - sniff passwords in network traffic

Password Selection Techniques

user education

- users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords

computer generated passwords

- users have trouble remembering them

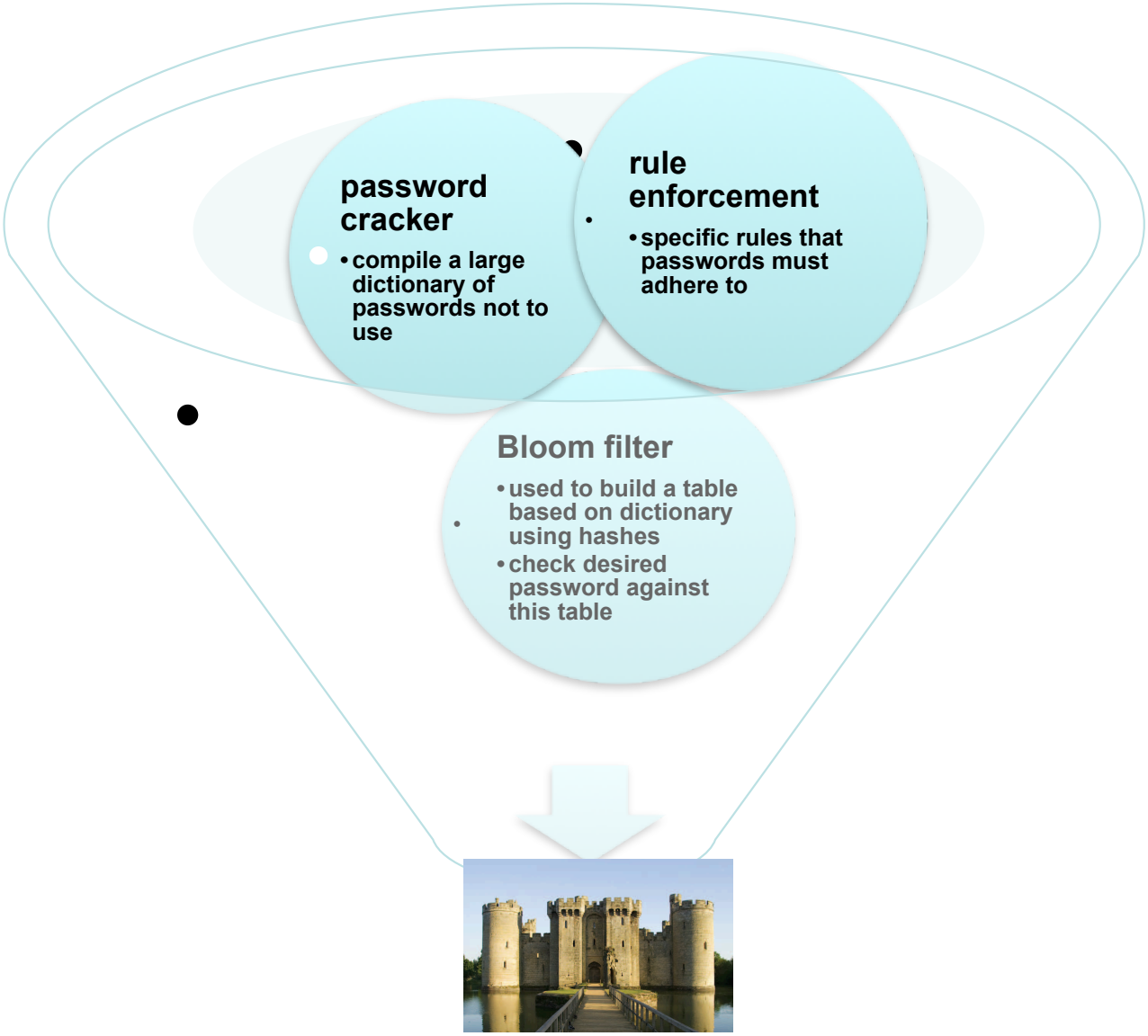
reactive password checking

- system periodically runs its own password cracker to find guessable passwords

proactive password checking

- user is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it
- goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking



Bloom Filters

- Probabilistic Data Structure using a bit map. Hash the word n times and place a 1 at bit index for each hash
- By definition, Bloom filter can check for if a value is **'possibly in the set'** or **'definitely not in the set'**..

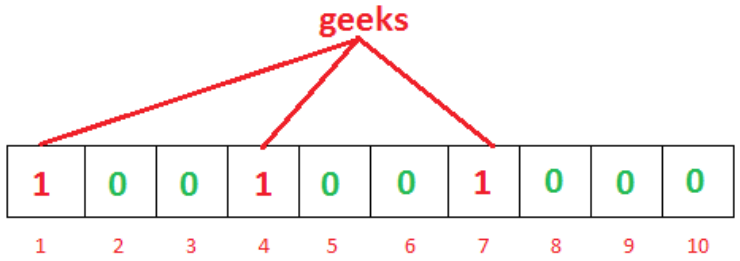


Image Credit: GeeksforGeeks

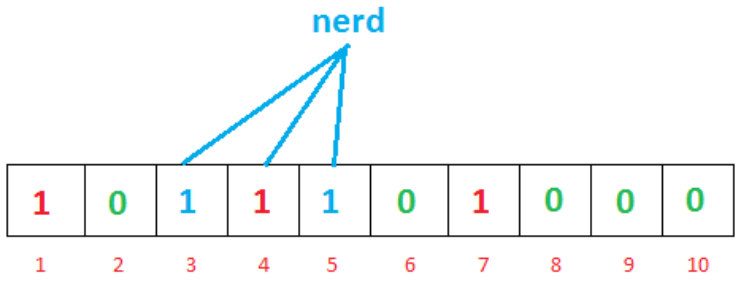


Image Credit: GeeksforGeeks

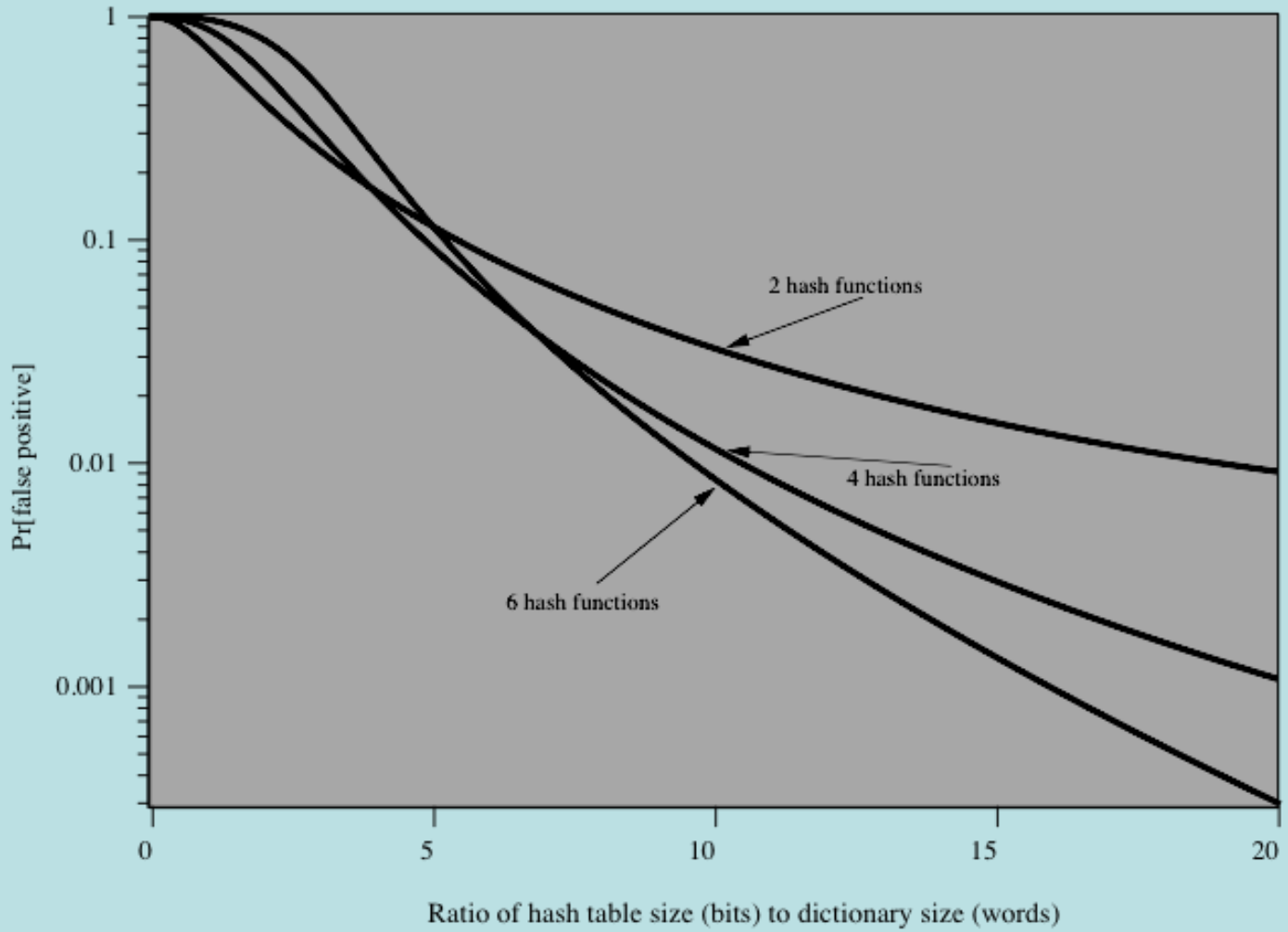


Figure 3.2 Performance of Bloom Filter

How big should the bit map be? How many hashes?

Suppose we have a dictionary of 1 million words and we wish to have a 0.01 probability of rejecting a password not in the dictionary. If we choose six hash functions, the required ratio is *R = 9.6.*

Therefore, we need a hash table of 9.6 x 10e6 bits or about 1.2 Mbytes of storage. In contrast, storage of the entire dictionary would require on the order of 8 MBytes. Thus, we achieve a compression of almost a factor of 7.

Furthermore, password checking involves the straightforward calculation of six hash functions and is independent of the size of the dictionary, whereas with the use of the full dictionary, there is substantial searching.

Other Authentication Methods

Tokens, Smart Cards, Biometrics