CS458: Introduction to Information Security

Notes 10: User Authentication

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

yelmehdwi@iit.edu

November 1st, 2018

Slides: Modified from Ewa Syta, Computer Security: Principles and Practice, 4th Edition. By: William Stallings and Lawrie Brown & Ari Juels and Vitaly Shmatikov

Outline

- A Story of Things Going Very Wrong
- User authentication
  - Password authentication, salt
  - Token-based authentication
  - Biometrics
- Remote User Authentication

The Weak Links: The case of Mat Honan 3 August 2012[1]

MAT HONAN GEAR 08.06.12 08:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

Meet Mat Honan. He just had his digital life dissolved by hackers.

PHOTO: ARIEL ZAMBELICH/WIRED. ILLUSTRATION: ROSS PATTON/WIRED

[1] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

The Weak Links: The case of Mat Honan 3 August 2012[2]

- 4:33 p.m., "Mat Honan" called AppleCare reporting lost me.com e-mail password. Apple issued temporary password.
  - "Mat" couldn't answer his own security questions.
  - Apple required only last four digits of a credit card and a billing address.
- 4:50 p.m.: Password reset e-mail arrived in Honan's me.com e-mail box; used to reset Honan's AppleID password
- 4:52 p.m.: GMail password recovery email arrived in Honan's me.com mailbox
- 4:54 p.m.: Honan's Google account password changed.

[2] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

The Weak Links: The case of Mat Honan 3 August 2012[3]

- 5:00 p.m.: iCloud "Find My" tool used to wipe Honan's iPhone
- 5:02 p.m.: Honan's Twitter password reset
- 5:05 p.m.: Honan's MacBook wiped
- 5:10 p.m.: The real Honan calls AppleCare
- 5:12 p.m.: Hackers post message on Honan's Twitter account taking credit for the hack

[3] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

How did it happen?

- Attackers started by compromising Honan's Amazon account
- Needed credit card number for Honan's Amazon account. How did they learn it?
- Attackers called Amazon and **added** a new credit card number to Honan's account. (Name, email, and billing address sufficed.)
- Attackers called Amazon to reset Honan's password. For identity verification, Amazon asked for a credit card number...

How did it happen?

- Once logged in to Honan's Amazon account, attackers learned last four digits of real credit card numbers
- "The very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers security enough to perform identity verification."

How did it happen?

- Then they called AppleCare...
- "It turns out, a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account. Once supplied, Apple will issue a temporary password, and that password grants access to iCloud."

The result?

- Honan hadn't backed up his data.
- He lost all of it, e.g., irreplaceable photos young daughter
- Why did hackers wipe his devices?
  - Just to prevent his regaining control of accounts!
- Honan got in touch with one of the hackers, Phobia, via instant messaging?
  - Quoth Phobia: "yea i really am a nice guy idk why i do some of the things i do."
  - "idk my goal is to get it out there to other people so eventually every1 can over come hackers"
  - "even though i wasnt the one that did it i feel sorry about that. Thats alot of memories im only 19 but if my parents lost and the footage of me and pics i would be beyond sad and im sure they would be too."

How The Hackers Did It - Defeating The Hackers - BBC

- Watch: How The Hackers Did It - Defeating The Hackers - BBC

User Authentication

- User Authentication is proving your identity to a system (or another person).
- i.e., the process of verifying that a user is who he or she claims to be.
  - The starting point of nearly any security protocol.
- Two phases of an authentication protocol:
  - Enrollment: the initial, one-time, sign-up process.
  - Authentication: the subsequent verification process.
- Distinct from Message authentication
  - Message authentication: is a procedure that allows communicating parties to verify that the content of a received message have not been altered, and that the source is authentic.

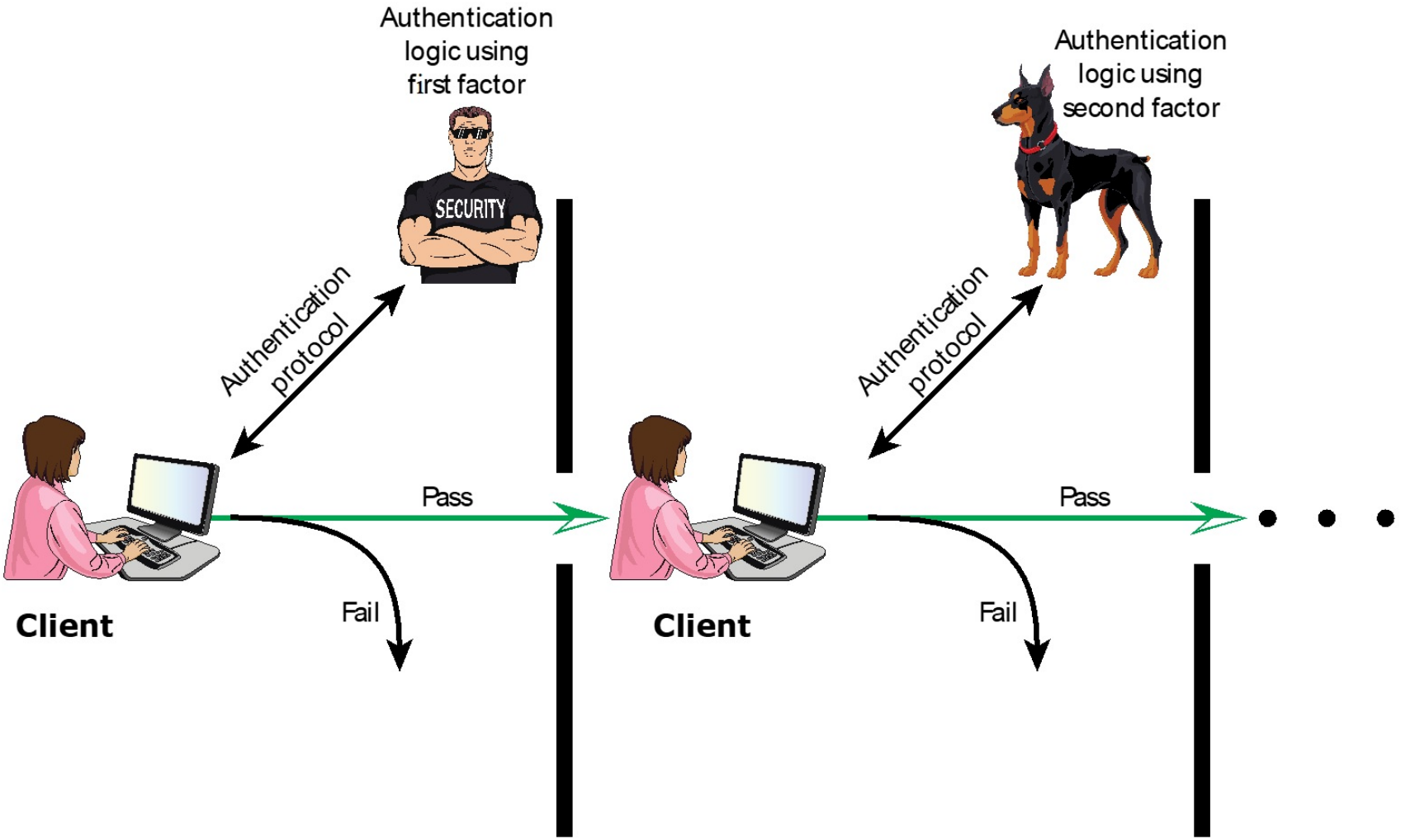
User Authentication Factors

- There are four factors/means of authenticating a user's identity
  - Something the individual knows (Knowledge-based)
    e.g. password, PIN, or answers to a prearranged set of questions.
  - Something the individual possesses (Possession-based)
    e.g. electronic keycards, smart cards, and physical keys. (referred to as a **token**)
  - Something the individual is (static biometrics).
    e.g. fingerprint, retina, and face
  - Something the individual does (dynamic biometrics)
    e.g. voice pattern, handwriting characteristics, and typing rhythm
- Can use alone or combined
- Can provide user authentication
- all have issues

Using Authentication Factors

- One, two, or even three factors can be required in order to authenticate a user
- Two-factor authentication is an approach which requires to present two different factors for authentication
- For example:
  - A password and a USB token
  - A fingerprint and a smart card
  - A credit card and a signature
- An increasingly popular approach. (More on that later).

Multifactor authentication



Password-Based Authentication

Something You Know: Passwords

- 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
- Lots of things act as passwords!
- For example:
  - PIN
  - Social security number
  - Mother's maiden name
  - Date of birth
  - Name of your pet, etc.

Trouble with Passwords

- "Passwords are one of the biggest practical security problems today"
- "Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

Why Passwords?

- Why is “something you know” more popular than “something you have” and “something you are”?
- i.e., why are passwords so popular?
  - The initial choice for authentication.
  - Cost: They are free.
  - Convenience: They are convenient (use & management)

Cryptographic keys vs. Passwords

- **Cryptographic keys**
  - Suppose a key is $128\text{-}bit$ long
  - 2^{128} possible keys
  - Keys are chosen at random
  - Attacker must try about 2^{127} keys.
- **Passwords**
  - Suppose passwords are 8 characters and 256 possibilities
  - Then, $256^8 = 2^{64}$ possible passwords
  - Users do not select passwords at random
  - Attacker needs to try far less than 2^{63} passwords (dictionary attack)

- Q: How do people pick their passwords?

Often they don't!

- In April 1994[4], English teenager ("Datastream Cowboy") penetrated Pentagon computers via the Air Force Rome (New York) Laboratory, started probing Korean nuclear facilities.
  - Deemed "No. 1 threat to U.S. military".
  - How did he do it?
    - Guessed default guest password!
- Surveys show that half of users leave the default password in place for their routers at home.
  - E.g., Warkitting: the Drive-by Subversion of Wireless Home Routers

[4] Hacking U.S. Government Computers from Overseas

Often they don't!

- Examples from Kevin Mitnick's Art of Intrusion
- NY Times employee database: pwd = last 4 SSN digits
- "Dixie bank": 99% of employees used password "password123"
- What's the most important thing in the world to prevent unauthorized access to?
  - Nuclear missiles!
    - From 1962 to 1977, the passcode for launching Minuteman missiles was 00000000[5].
    - Strategic Air Command was more afraid of lost passwords than of Armageddon!

[5] Source of the reports was former ICBM launch officer Bruce Blair

Good and Bad Passwords

- **Bad passwords**
  - frank
  - Fido
  - Password
  - incorrect
  - Pikachu
  - 102560
- **Good passwords**
  - jflej,43j-EmmL+y
  - 09864376537263
  - P0kem0N
  - FSa7Yago
  - 0nceuP0nAt1m8
  - PokeGCTall150
- Q: How would you define a good password?

Most popular passwords[6]

1. 123456 (Unchanged)
2. Password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 2)
5. 12345 (Down 2)
6. 123456789 (New)
7. letmein (New)
8. 1234567 (Unchanged)
9. football (Down 4)
10. iloveyou (New)
11. admin (Up 4)
12. welcome (Unchanged)
13. monkey (New)
14. login (Down 3)
15. abc123 (Down 1)
16. starwars (New)
17. 123123 (New)
18. dragon (Up 1)
19. passw0rd (Down 1)
20. master (Up 1)
21. hello (New)
22. freedom (New)
23. whatever (New)
24. qazwsx (New)
25. trustno1 (New)

[6] The 25 Most Popular Passwords of 2017: You Sweet, Misguided Fools

Getting passwords right is difficult

- You need to balance security and convenience.
  - Weak passwords easy to remember.
  - Strong passwords difficult to remember
- Password Do's and Don'ts
  - Choose long passwords with special characters.
  - Use passphrases to remember passwords:
    "It was a dark and stormy night" $\rightarrow$ `iWadasn`
  - Don't use dictionary words or personal information.
  - Don't reuse passwords
- ... but user compliance is extremely difficult.

Attacks on Passwords

- Attacker could
  - Target one particular account.
  - Target any account on system.
  - Target any account on any system.
  - Attempt denial of service (DoS) attack
- Common attack path
  - Outsider $\rightarrow$ normal user $\rightarrow$ administrator (privilege escalation attack)
  - May only require one weak password!

Password Vulnerabilities

- Offline dictionary attack
  - The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination.
- Specific account attack
  - The attacker targets a specific account and submits password guesses until the correct password is discovered.
- Popular password attack
  - A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs.
- Password guessing against single user
  - The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password
- Workstation hijacking
  - The attacker waits until a logged-in workstation is unattended

Password Vulnerabilities

- Exploiting user mistakes
  - If the system assigns a password, then the user is more likely to write it down because it is difficult to remember.
  - A user may intentionally share a password, to enable a colleague to share files, for example.
  - Attackers trick the user/account manager into revealing a password.
  - Many computer systems are shipped with preconfigured passwords for system administrators. Unless these preconfigured passwords are changed, they are easily guessed.
- Exploiting multiple password use
  - Attacks can also become much more effective or damaging if different network devices share the same or a similar password for a given user.
- Electronic monitoring
  - If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping.

Countermeasures

- stop unauthorized access to password file
- intrusion detection measures
- account lockout mechanisms
- policies against using common passwords but rather hard to guess passwords
- training & enforcement of policies
- automatic workstation logout
- encrypted network links

Password retry

- Usernames are either public or easily guessable. It makes a brute force attack possible.
- **Common response**: Account lockout mechanism lock account after `X` tries for `Y` minutes
  - What `X` and `Y` should be?
  - Again, security vs. convenience.

Forgotten passwords

- What happens when you forget your password?
- Users forget passwords and need a way to recover them.
  - Email reset
    - Risks exemplified by Mat Honan's story
  - Personal questions
    - Also called "security questions," "personal knowledge questions," or "life questions"
    - Another something-you-know factor
  - Sometimes a combination of these options
- Security questions
  - Might be an easier way for an attacker to obtain access to an account than guessing a password.
  - What is your favorite color? Sport? Team?
- **Read and submit a summary for extra credit:)**: Personal Information Leakage During Password Recovery of Internet Services

Sarah Palin's password recovery[7]

- On 16 Sept. 2008, then Gov. Palin's Yahoo! account was hacked. How?
  - Password reset
    - Zip code?
    - *Only 2 in Wasilla*
    - Date of birth?
    - *Wikipedia: February 11, 1964*
    - Where did you meet your spouse?
    - *Wikipedia: met Todd in high school...*
- Password posted to /b/ on 4chan.
- When everyone tried to log into Palin's account, Yahoo! finally detected attack
- 20-year-old hacker David Kernell (a.k.a. Rubico) caught
  - Sentenced to one year of federal prison

[7] Palin e-mail hacker says it was easy

Problems with security questions

- Answers easy to guess or find out
  - Attackable using public records, LinkedIn, etc.!
- Answers hard to remember find out
  - People lie to increase security...then forget their answers.

Storing passwords

- Passwords must be stored on the server for verification.
  - Plaintext: Once Eve gets access, she gets all passwords.
  - Encrypted: Where is the key stored?
  - Better solution: Use a hash function!
- Hashing passwords
  - **Enrollment**
    - Alice sends her password.
    - Bob stores $y = h(password)$.
  - **Authentication**
    - Can verify entered password by hashing
    - Alice sends her password
    - Bob calculates $y' = h(password')$ and checks if $y = y'$

Hashing passwords

- Once Eve gets in, she only gets hashes of passwords
  - i.e., she obtains the password file, she does not (directly) obtain passwords
  - Crypto hash functions are one-way.
  - Brute force?
- Cracking passwords
  - Eve can try a forward search.
    - Guess x and check whether $y = h(x)$.
  - But x does not have to be guessed at random

Dictionary Attack

- We're bad at choosing good passwords.
  - Develop a large dictionary of possible passwords and try each against the password file
  - Eve pre-computes $h(x)$ for all x in a dictionary of common passwords.
- Attack: Eve gets access to a hashed password file.
  - She only needs to compare hashes to her pre-computed dictionary.
  - After one-time work of computing hashes, actual attack is trivial.
- Brute force attack
  - Try every possible combination of characters against the hashed password
  - Time taken increases exponentially as password length and key space increases.

Rainbow tables

- trade off space for time by precomputing tables of potential hash values
- a mammoth table of hash values
- e.g. 1.4GB table cracks 99.9% of alphanumeric Windows passwords in 13.8 secs
- lots available online[8]

- Can we prevent this forward search attack? Or at least make it more difficult?

[8] RainbowCrack Project: List of Rainbow Tables

Cracking Protection: Salt

- Salting requires adding a random piece of data and to the password before hashing it.
- Hash passwords with salt in order to randomize them.
- Choose a random salt s and compute $y = h(password, s)$ and store (s, y) in the password file.
- Note that the salt s is not secret
  - Analogous to IV.
- Still easy to verify salted password. But lots more work for Eve.

Password Cracking Tools

- (Some) popular password cracking (aka password auditing) tools[9]
  - Password Crackers
  - Cain & Abel (Windows)
  - John the Ripper (Unix)

- Admins should use these tools to test for weak passwords since attackers will.

- ... and they're getting faster
  - Custom GPU-based hardware
    - A 5-server rig with 25 Radeon GPUs
    - 77 million md5crypt-hashed passwords per second
  - Cloud-based cracking tools
- Good articles on password cracking
  - Password Crackers - Ensuring the Security of Your Password
  - Passwords revealed by sweet deal

[9] Wondershare, Top 10 Password Cracking Tools

Modern Approaches

- Complex password policy concept:
  - Users are doing a better job of selecting passwords, and organizations are doing a better job of forcing users to pick stronger passwords
- However password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use
    - numerous sets of leaked password files have become available for analysis.

Other Password Issues

- Too many passwords to remember.
  - Results in password reuse.
  - Q: Why is this a problem?
- Other issues:
  - Failure to change default passwords.
  - Social engineering & phishing.
  - Error logs may contain passwords.
  - Bugs, keystroke logging, spyware, etc.
  - Users might intentionally share passwords!

Other Password Issues: ... and some exotic ones

- E.g., reflections
  - iSpy: automatic reconstruction of typed input from compromising reflections

Figure 1: Some example threat scenarios that we investigated. Video was recorded in both indoor and outdoor environments, using various consumer video cameras. top: shoulder surfing, bottom: reflection surfing, bottom right: key *pop-out* event.

Other Password Issues: ... and some exotic ones

- Vibrations
  - (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers

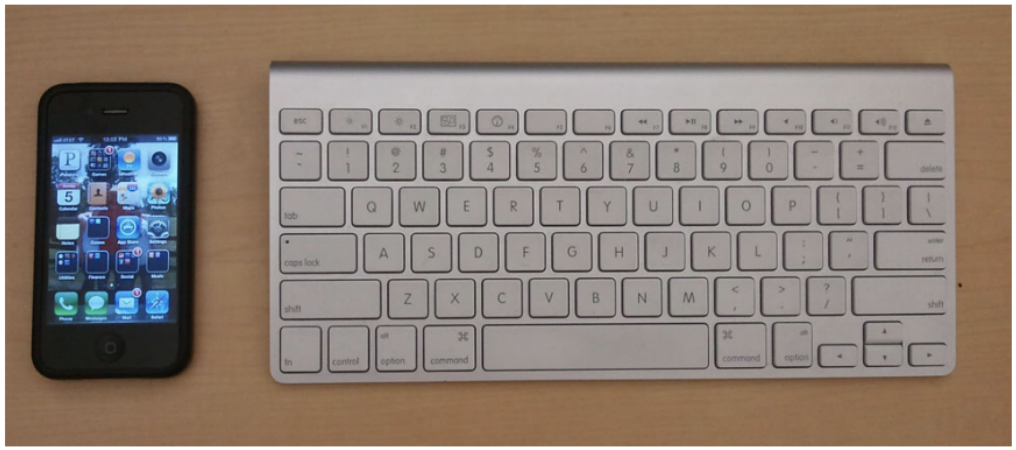


Figure 1: Our experimental placement of a mobile phone running a malicious application attempting to recover text entered using the nearby keyboard.

Passwords leaks

- 1.4 Billion Clear Text Credentials Discovered in a Single Database
- 5 Million Google Passwords Leaked Source
- 10000 Twitter User Accounts Exposed

Password File Access Control

- One way to thwart a password attack is to deny the opponent access to the password file
- Can block offline guessing attacks by denying access to encrypted passwords
- Make available only to privileged users
- Often, the hashed passwords are kept in a separate file from the user IDs, referred to as a shadow password file
- Still have 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 Strategies

- 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
- Complex password policy/proactive password checker
  - A promising approach to improved password security
  - User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it
  - i.e., don't let the user pick a "bad" password in the first place
  - Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking

- Rule enforcement
  - Specific rules that passwords must adhere to
  - Can be automated by using a proactive password checker, such as the password/passphrase strength checking and policy enforcement toolset
- Password checker
  - Compile a large dictionary of possible "bad/not to use" passwords
  - When a user selects a password, the system checks to make sure that it is not on the disapproved list
  - Time and space issues. Need to have a fairly fast test of the "goodness" of a password
- Markov Model
  - Generates guessable passwords
  - Hence reject any password it might generate
- Bloom filter:
  - Used to build a table based on hash values
  - Check desired password against this table

One password defense: 1- Password expiration (password changes)

- Common interval: 90 days
- May help sometimes, but
  - Helps users forget passwords
    - Estimated $150 cost per user per year
    - META group estimate: 1.75 help desk calls a month;
    - Gartner group: 30% of calls are for password resets;
    - Forester research: $25 / call
- Password-reset questions, social engineering, etc., come into play...

1- Password expiration (password changes)

- How do users change their passwords[10]?
  - `Password1`
  - `Password2`
  - `Password3`
  - `Pa$sword1`

[10] The security of modern password expiration: an algorithmic framework and empirical analysis

2- Password managers

- Why should users have to remember passwords?
- Password managers solve this problem.
  - LastPass, RoboForm, Dashlane, KeePass, etc
- Idea: Encrypt all of your passwords under a single, master password
- One password to rule them all

Passwords

- The bottom line... Password attacks are too easy.
  - Often, one weak password will break security.
  - Users choose bad passwords
  - Social engineering attacks, etc.
- Eve has (almost) all of the advantages.
- Passwords are a BIG security problem.
  - And will continue to be a problem.
  - Passwords are not going to disappear anytime soon.
  - Solution: Password managers?
- What is Your Password?

- Something You Have: Token-based Authentication

Something You Have: Token-based Authentication

- Something in your possession. You need to prove the possession of the factor in order to authenticate.
- Objects that a user possesses for the purpose of user authentication are called tokens
  - Car key
  - Laptop computer (or MAC address)
  - Cell phone
  - (One-time) Password generator
  - ATM card, smart card, etc.

Security Tokens[11]

- A security token is a physical device used to gain access to an electronically restricted resource.
- The token is used in addition to or in place of a password

[11] Source: Wikipedia: Security Tokens

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
  - Magnetic stripe can store only a simple security code, which can be read (and unfortunately reprogrammed) by an inexpensive card reader
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

Smart Cards

- Has the appearance of a credit card
- Has an electronic interface
- Has own processor, memory, I/O ports
- wired or wireless access by reader
- executes protocol to authenticate with reader/computer
- also have USB dongles
- **Authentication options**
  - Static: user authenticates herself to the token and then the token authenticates the user to the computer
  - Dynamic password generator: the token generates a unique password periodically (e.g., every minute).
  - Challenge response:
    - Computer system generates a challenge, such as a random string of numbers.
    - The smart token generates a response based on the challenge.

Two-Factor Authentication in practice

- Two-Factor == Two-Step
- Two most popular options: email and cell phone (apps or text msgs)
- Pretty much all major websites offer two-factor authentication.
  - LinkedIn, Twitter, Microsoft, Apple, Google, Dropbox, Tumblr, Snapchat, Instgram, etc.

Something you are: Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

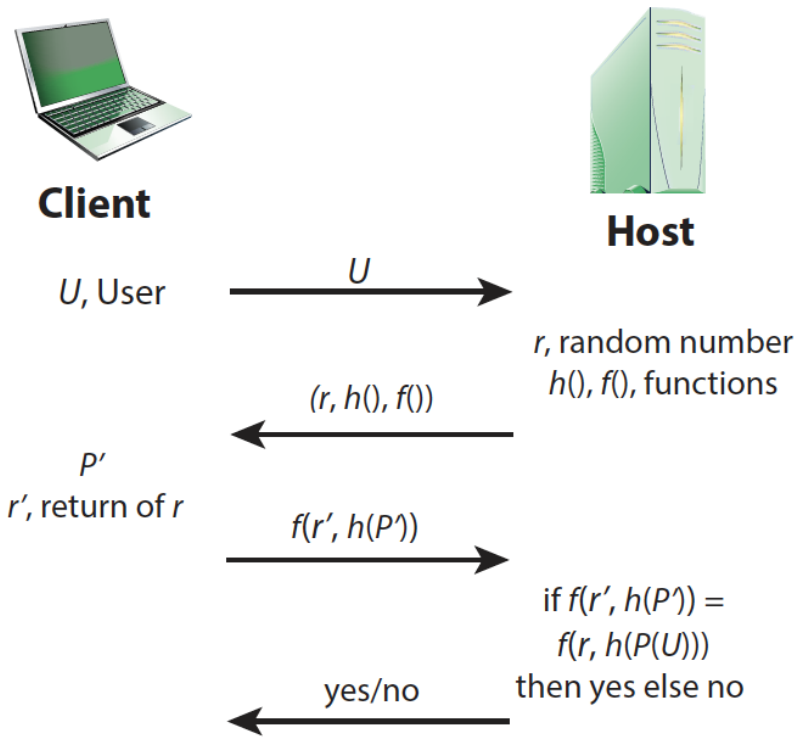
Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally rely on some form of a challenge-response protocol to counter threats

Remote User Authentication: Password protocol

- User transmits identity to remote host
- Host generates a random number r (**nonce**) and returns it to the user
- In addition, host specifies two functions $h()$ (hash function) and $f()$ to be used in the response
- This transmission from host to user is the challenge
- User's response: $f(r', h(P'))$, where $r'=r$ and P' is the user's password
- Host stores a hash function of each registered user's password
  - $h(P(U))$ for user U
- Host compares $f(r', h(P'))$ to the calculated $f(r, h(P(U)))$
  - If match, the user is authenticated.

Password protocol



Kerberos protocol[12]Kerberos: The Network Authentication Protocol

- In security, Kerberos is an authentication protocol based on symmetric key crypto
  - Originated at MIT
  - Has been issued as an Internet standard and is the de facto standard for remote authentication
  - Relies on a Trusted Third Party (TTP)

[12] https://web.mit.edu/kerberos/

Motivation for Kerberos

- Authentication using public keys
  - $\mathtt{N}$ users $\rightarrow$ $\mathtt{N}$ key pairs
- Authentication using symmetric keys
  - $\mathtt{N}$ users requires (on the order of) $\mathtt{N}^2$ key pairs
- Symmetric key case does not scale
- Kerberos based on symmetric keys but only requires $\mathtt{N}$ keys for $\mathtt{N}$ users

  \- Security depends on TTP

  \+ No PKI is needed

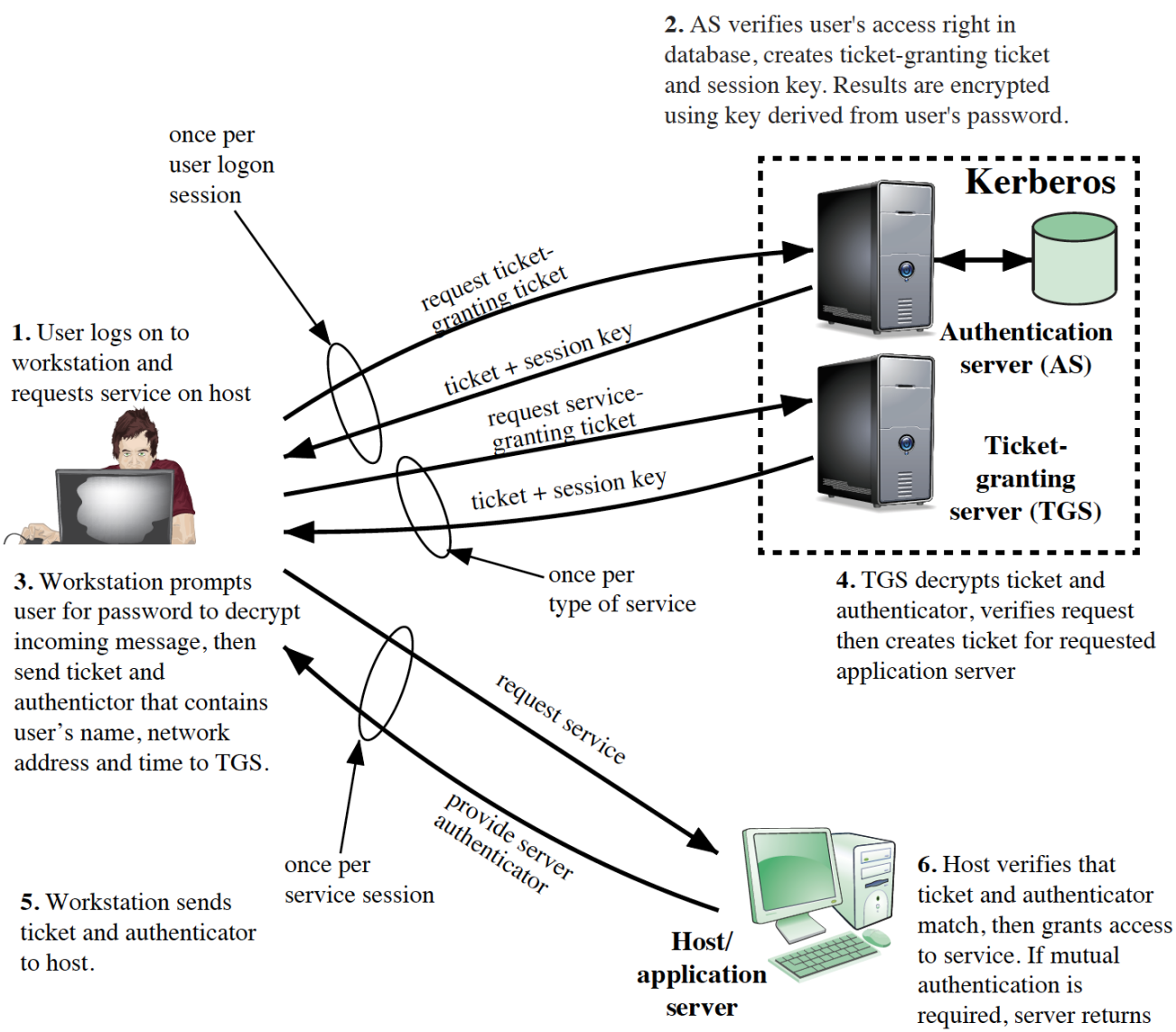
Kerberos

- Users wish to access services on servers.
- Three threats exist:
  - User pretend to be another user.
  - User alter the network address of a workstation.
  - User eavesdrop on exchanges and use a replay attack.

Kerberos

- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

Overview of Kerberos



Key Points

- Passwords are the reality for now
- Multi-factor authentication is must stronger
- Biometrics can help, but not a silver bullet yet