Implementation and Management of Systems Security

158.738

A/Prof. Julian Jang-Jaccard
Massey University

PERSONAL SECURITY

User Authentication

- Ensure that only the authorized users;
  - Are permitted into network
  - allowed into the specific resources
- Basis of user authentication: 3 factors
  - Something you know
  - Something you have
  - Something you are
- Can used alone or in combination, for example two factor authentication
  - Something you know (PIN) + Something you have (bank card)

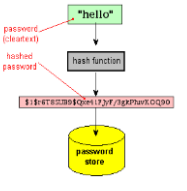
Something you know

- Password based
  - Users gain access based on something they know
  - Should be long and complex
  - Easy to recall
  - Unique
- Password Weaknesses
  - Not very secure due to poor choice of passwords
  - Because human beings can memories only a limited number of items
  - Security policy enforcement doesn't help
  - Produce weak passwords

Ten most used passwords

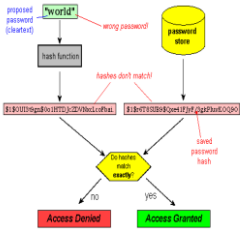
Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Loading password



- User supplies password
- Hash applied to combination of password
- Often Salt (i.e., pseudorandom or random number) is added to the hash to increase attacker workload by increasing the complexity of the hash
- Store userID, hash in the password file
- Password is not stored!
- Password files often hidden (shadow passwords in Unix, only accessible to system admin)

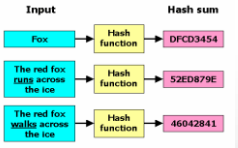
Verifying password



- User provides their ID and password.
- Lookup the hash.
- Recompute the hash using the supplied password
- Does the recomputed hash equal to what was expected?
- Note that this scheme never reveals the password to anyone, even to system admin

Hash Function

- It's a ONE-WAY function
  - Takes a variable-length string as input
  - Returns a fixed-length string as output
- Even a small change in the input drastically changes the output



Hash functions

- Popular hash function MD5
  - Produce 128 bit ciphertext
  - E.g., b9b985cdc61c8db72289ce54f0937eb2 (32 hex)
  - Thoroughly broken
- Government standard SHA-1, SHA-2
  - SHA-1 : 160 bit ciphertext
  - E.g., 14751031b69d5480dfb30023f72640dd45a3c5de (40 hex)
  - Theoretical weaknesses
- "NEW" cryptographic hash function SHA-3
  - Too new to fully evaluate
  - Maybe good enough

Attacks on Passwords

- Brute force Attack
  - Attempt on every possible combination of letters, numbers, and characters
  - Create candidate digests (called rainbow table) for matching
  - Computation intense
- Dictionary Attack
  - Begins with creating digests of common dictionary words or their mutations
  - e.g. p@ssw0rd, Luv4Eva
  - Intelligent cracker tool will apply those mutations automatically

Social Engineering

- A means of manipulating users to perform an action or gather confidential information
  - Relies on the actions of the victims (not rely directly on technology)
- Also referred as People Hacking
  - People are the weakest link in any security system.
  - *"Only amateurs attack machines; professionals target people." Bruce Schneier*
  - "People hacking".
  - *Exploits people's trusting nature.*
  - Hardest thing to defend against.

Social Engineering Techniques

- Pretexting: inventing false (yet believable) stories (e.g., Nigerian scam)
- Typo Squatting: rely on typo goggle.com instead of google.com
- Hoaxes: false warning such as deadly virus
- Dumpster Diving: digging through trash receptacles
- Shoulder Surfing: observing victim's action

Role of Internet

- Previously one-to-one interaction, now one-to-many via email or social media platforms
- Larger number of marks means larger absolute number of marks who fall for the scam
- People find it hard to make trust judgements in the absence of body language and other signals that you get in a one-to-one interaction

Identity Theft

- Involves using someone's personal information to commit financial fraud
  - Obtain a credit card then remove all money from the bank account
  - Establish phone or wireless service in the victim's name
  - Going on spending sprees
  - Obtain loans for expensive items
  - Filing fictitious income tax returns
- The victim is charged for the purchases & loose reputation

Password Security

- General Rules for creating Strong Passwords:
  - Do not use passwords that consist of dictionary words
  - Do not repeat characters (xxx) or use sequences (abc, 12s, qwerty)
  - Do not use birthdays, family & pet names, addresses or any personal information
  - Longer is better – current recommendation is 18 or more
  - Don't use the same passwords everywhere
  - Always choose a unique password for every high-risk site, such as your bank
  - Use passphrases, not passwords.

Schneier Scheme

- Take a sentence and turn it into a password (along with digits, lower-case, upper-case, and special characters)
  - WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
  - Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
  - Wow...doestcst = Wow, does that couch smell terrible.
  - uTVM,TPw55:utvm,tpwstillsecure = Until this very moment, these passwords were still secure.

Password Managers

- Password generators
  - Generates strong passwords on behalf of the users.
  - Where to save them?
- Online vaults
  - Instead of creating the user's password each time, it retrieves the password from a central online repository.
  - Vulnerable to attackers
- Password Management Applications
  - User can create and store multiple strong passwords in a single user "vault" file.
  - The personal vault is protected by one strong master password
  - KeePass Password Safe, LastPass

Something you have

- Something human owns that can authenticate the holder
  - Smart cards, Security hardware tokens
- Users gain access based on something they have

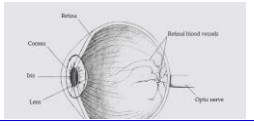



Example: Smart Card

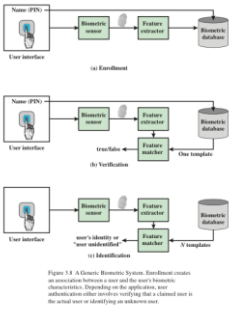
- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
  - Same technology could support different services etc.
- Contain:
  - An entire microprocessor, Processor, Memory, I/O ports (connected to radio or connector)
- Typically include three types of memory:
  - Read-only memory (ROM)
    - –Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM)
    - –Holds application data and programs
  - Random access memory (RAM)
    - –Holds temporary data generated when applications are executed

Something you are (Biometric)

- Users gain access based on something they are
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Becoming more common due to fingerprint readers etc. being built into mobile phones
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice



Biometric: how it works



- Pattern recognition.
- Face: relative location and shape of key facial features.
- Fingerprint: furrows and ridges.
- Hand geometry: shape, lengths and widths of fingers.
- Retinal pattern: veins illuminated by low-intensity beam of light.
- Signature: writing habit, pressure, shape of signature
- Voice: based on anatomy and physical characteristics
- *NOT 100% ACCURATE UNLIKE A PASSWORD*

Central Authentication

- Also called single sign-on
  - Allows users to access multiple services with a single login
  - Provides a single access to multiple systems within a single organisation
- Phase 1: Requires user to login to an authentication server
  - Checks id and password against a database, then a certificate
- Phase 2: Certificate used for all transactions requiring authentications
  - No need to re-enter passwords, Eliminates passwords changing hands

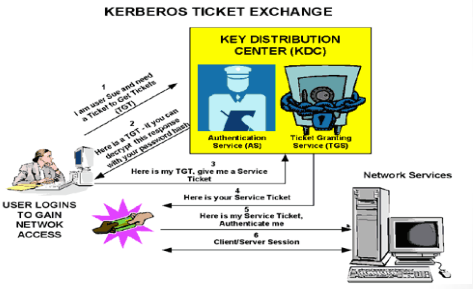
Kerberos

- Most commonly used authentication protocol
- In Greek mythology, kerberos is a multi-headed dog (usually three) which guards the entrance of Hades
- Kerberos is an authentication server that acts as a third party authenticator
  - Helps the user to prove its identity to the various services

Kerberos

- What with the 3 heads?
  - Authentication: Confirms that a user who is requesting services (user credential)
  - Authorization: Granting of specific types of service to a user based on their authentication (ticket)
  - Accounting: The ticketing of the consumption of network resources by users

Kerberos at work



https://msdn.microsoft.com/en-us/library/bb742516.aspx

OAuth

- Moving enterprise authentication server to Web
- Called as HTTP-based Single Sign-On
  - Similar in spirits with Kerberos, OpenID, SAML
- Strictly speaking, it's a Federated Identity
  - Provides a single access to multiple systems across multiple organisations
- Open Standard allows Internet users to log in to 3rd party websites
  - Sign their accounts at Google, Facebook etc.,

OAuth example

OAuth Benefits

- Authorization and Authentication provided by third party Service Provider
  - Application developers can focus on building an app, not an authentication framework
- Username and password are not processed by application
  - User identification is collected by service provider
  - Improves Usability and Security
- Centralized management of user accounts
  - Users don't need to create separate account for each application/service
  - Fewer identities & passwords to remember

OAuth Service Provider

- For web access to Google APIs Google
  - Google+, Drive, AdSense, Analytics, and many more...
- Web and Streaming (real time) APIs twitter
- Using Graph API (ie a low-level HTTP-based API) to get data in and out of Facebook's platform facebook

OAuth Clients

- Websites
  - CNN, Washington Post, Gawker, Kickstarter, La Crosse Tribune, etc.
- Mobile apps & games
  - According to Facebook, 81 of the top 100 grossing iOS apps and 62 of the top 100 grossing Android apps use Login with Facebook
- Anything with a "Log in with Facebook/ Google +/Twitter" option

END