Principles of Computer Security

Alvin Lin

January 2018 - May 2018

Authentication and Access Control

Authentication Process:

- Basis for access control and user accountability
- "The process of verifying an identity claimed by or for a system entity" (RFC 4949)
- Involves an indentification step (presenting an identifier to a security system) and a verification step (presenting or generating identification information to corroborate binding between the entity and identifier)

Means of Authentication User Identity

Aspect	Example
Something an individual **knows**	Password, PIN, answers to prior questions
Something an individual **possesses** (token)	Smart card, electronic keycard, physical key
Something an individual **is** (static biometrics)	Fingerprint, retina, face
Something an individual **does** (dynamic biometrics)	Voice pattern, typing rhythm, handwriting

Password Authentication

Password authentication is a widely used line of defense against intruders where the user provides a name/login and password. The system compares the password with

the one stored for that specified login. The user ID checks if the user is authorized to access the system, determines the privileges, and is used in discretionary access control. A widely used password security technique involves using hashed passwords and a salt value.

Password Vulnerabilities

- Offline dictionary attack
- Specific account attack
- Popular password attack
- Password guessing against a single user
- Workstation hijacking
- Exploiting user mistakes
- Exploiting multiple password use
- Electronic monitoring

Password Cracking

Dictionary attacks:

- Keep a set of possible passwords and try each against 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
- Countered by a sufficiently large salt value and a hash length

Password crackers exploit "people choose guessable passwords":

- Shorter password lengths are also easier to crack

John the Ripper:

- Open-source password cracker first developed in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

Complex password policies force users to pick stronger passwords. But password-cracking has also improved. We have increased processing capacity for password cracking, sophisticated algorithms to generate likely passwords, and we can study examples and structures of actual passwords. GPUs now allow password-cracking programs to work thousands to times faster than just a decade ago.

Password File Access Control

We can block offline guessing attacks by denying access to encrypted passwords. They should be made available only to privileged users and shadow password file. Vulnerabilities:

- Weakness in 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

Users can be told or compelled to choose strong passwords. Users have trouble remembering computer generated passwords. Systems can also periodically run their own password crackers to find guessable passwords. Complex password policies allow users to select their own passwords, but the system checks if the password is acceptable and will reject it otherwise.

Identification Methods

- Smart Tokens: Physical tokens that include an embedded microprocessor. Authenticates a user with a static key, a dynamic password generator, or a challenge-response method. This provides a stronger proof of identity if it is government issued for a variety of applications.
- Biometric Authentication: Attempts to authenticate an individual based on unique physical characteristics. This can be done through pattern recognition, facial recognition, fingerprints, retinal patterns, voice patterns, etc. It is technically complex and more expensive compared to passwords and tokens.
- Remote User Authentication: Authenticates a user over a network. This is vulnerable to additional security threats such as eavesdropping and password capture. A challenge-response protocol is usually needed to counter threats.

Authentication Security Issues

- Eavesdropping: tries to learn a password by an attack that involves physical proximity of a user and adversary.
- Host Attacks: directed at user files on the host containing passwords, tokens, and biometric templates.
- Replay: tries a previously captured user response.
- Client Attacks: tries user authentication without access to the remote host or the communications path.
- Trojan Horse: masquerades as an authentic application or device for capturing a user password.
- Denial-of-Service: attepts to disable a user authentication service by flooding the service with numerous authentication attempts.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech