Notes Oct 4 2018

Table 3.1 Identification and Authentication Security Requirements (SP 800-171)

* Basic Security Requirements:
  + Identify information system users, processes acting on behalf of users, or devices.
  + Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
* Derived Security Requirements
  + Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
  + Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
  + Prevent reuse of identifiers for a defined period.
  + Disable identifiers after a defined period of inactivity.
  + Enforce a minimum password complexity and change of characters when new passwords are created.
  + Prohibit password reuse for a specified number of generations.
  + Allow temporary password use for system logons with an immediate change to a permanent password.
  + Store and transmit only cryptographically-protected passwords.

Figure 3.1 The NIST SP 200-63-2 E-Authentication Architectural Model

* Registration, Credential Issuance, and Maintenance
  + Registration Authenticy

The four means of authenticating user identity are based on:

* Something the individual knows
  + Password, PIN, answers to prearranged questions.
* Something the individual possesses

Figure 3.2 multifactor Authentication

* Client 🡨🡪 Authentication logic using first factor 🡨🡪 Authentication logic using second factor
* Client 🡪Pass 🡪

Risk Assessment for User Authentication

* There are three separate concepts:

Assurance Level

* Describes an organization’s degree of certainty that a user has presented a credential that refers to his or her identity.
* More specifically is defined as:
  + The degree of confidence in the vetting process and to establish the identity of the individual to whom the credential was issued.

Potential Impact

* FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
  + Low
    - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
  + Moderate
    - An authentication error could be expected to have a serious adverse effect
  + High
    - An authentication error could be expected to have a severe or catastrophic adverse effect.

Table 3.2

* Assurance Level Impact Profile.
* Potential Impact Categories for

Password Vulnerabilities

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

Figure 3.3 UNIX Password Scheme

* Password Password File Salt User ID Salt Hash Code allow hash function Load Loading a new password
* User id Passwrod File User ID Salt Hash code select salt show hash function Password compare verifying a password.

UNIX Implementation

Improved Implementations

* Much stronger hash / salt schemes available for Unix 🡪 recommended hash function is based on MD5
  + Salt of up to 48-bits
  + Password length is unlimited
* OpenBSD uses Blowfish block cipher based hash algorithm called

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 a hash values.
* Rainbow table attacks

Modern Approaches

* Complex password policy
  + Forcing users to pick stronger passowrds
* However password-cracking techniques have also improved
  + The processing capacity available

Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

Password File Access Control

* Can block offline guessing attacks by denying access to encrypted passwords.

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

Proactive Password Checking

* Rule

Figure 3.5 Performance of Bloom Filter.

Table 3.3

* Card Type – Defining Feature – Example
* Embossed – Raised

Memory Cards

* Can store but do not process data
* The most common is the magnetic stripe card
* 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 Tokens

* Physical characteristics:
  + Include an embedded

Figure 3.6 Smart Card / Reader Exchange

* Smart Card 🡪 Card reader
* Smart Card Activation
* 🡨 ATR

Electronic Identity Cards (eID)

* Use of a smart card as a national identity card for citizens.

Figure 3.7 User Authentication with eID

Password Au

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.

Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

* Iris, Hand, Retina, Signature, Finger, Face, 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.

Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

* Client Host Client Host Client Host Client Host

Table 3.5

* Some Potential Attacks, Susceptible Authenticators, and Typical Defenses
  + Attacks Authenticators Examples Typical Delusion
  + Client Attack Password Guessing,

Attacks on Passwords

* Attacker

Password Retry

* Suppose system locks after 3 bad passwords. How long should it lock?
  + 5 seconds
  + 5 minutes
  + Until SA restores service
* What are +’s and –‘s of each

Password File?

* Bad idea to store passwords in a gile
* But we need

Salt

* Hash password with salt
* Choose random salt s and compute y = (password,s)

Password Cracking: Case I

Password Cracking: Case III

Kerberos Overview

What is Kerberos

* Network authentication protocol.
* Developed at MIT in the mid 1980s
* A secret key
* Authentication is a key feature in multi-user
* Sending usernames and passwords in the clear text jeopardizes the security of the network
* Each time a password is sent in the clear text, there is a chance for interception.
* Firewalls make a risky assumption: that

Kerberos Model

* Kerberos
* Encry
* Three basic functions (message exchanges)

Functions

Kerberos Functionality

* Instead of client sending password to application server:
  + Request tickets from authentication server
  + User presents a ticket that is issued to it by a Kerberos Authentication Server(AS).
  + If the ticket is valid

Kerberos Overview

Drawbacks of Kerberos

* Single point of failure: It requires continuous availability of a central server. When the

Conclusion

* Authentication is critical for the security of computer systems. Without knowledge of the identity of the principal requesting an operation, it’s difficult to decide whether.