UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

Lecture 11: Authentication and Account Management

Objectives

- Describe the three types of authentication credentials
- Explain what single sign-on can do
- List the account management procedures for securing passwords
- Define trusted operating systems

Authentication

- Process of ensuring a person desiring to access resources is authentic
- Chapter topics
  - –Authentication and secure management of user accounts
  - –Different types of authentication credentials
  - –Single sign-on
  - –Techniques and technology to manage user accounts securely
  - –Trusted operating systems

Authentication Credentials

TYPES OF AUTHENTICATION CREDENTIALS

What you know

Example: password

What you have

Example: id badges

What you are

Example: fingerprints, face recognition, iris scans, hand geometry

What You Know: Passwords

- User logging in to a system
  - –Asked to identify himself
- User enters username
  - –User asked to authenticate
- User enters password

- Passwords are most common type of authentication today
- Passwords provide only weak protection

PASSWORD WEAKNESSES

- Users must remember passwords for many different accounts
- Each account password should be unique

Weakness of passwords is linked to human memory
–Humans can only memorize a limited number of items
–Long, complex passwords are most effective
•Most difficult to memorize

Security policies mandate **passwords must expire**
–Users must repeatedly memorize passwords

Users often take shortcuts
–Using a weak password Examples: common words, short password, or personal information
–Reuse the same password for multiple accounts
•Easier for attacker who compromises one account to access others

What You Know: Passwords

ATTACKS ON PASSWORD

Social engineering
–Phishing, shoulder surfing, dumpster diving

Capturing
–Keylogger, protocol analyzer
–Man-in-the-middle and replay attacks

Resetting
–Attacker gains physical access to computer and resets password

Online guessing
–Not really practical

Offline cracking
–Method used by most password attacks today
–Attackers steal file with encrypted password
•Compare with encrypted passwords they have created

Offline cracking types

Brute force
•Every possible combination of letters, numbers, and characters used to create encrypted passwords and matched against stolen file
•Slowest, most thorough method

Passwords Defenses

PASSWORD COMPLEXITY

- Creating strong passwords
  - Insight into how to create strong passwords gained by examining attack methods
- Most passwords consist of:
  - Root (happy, graduate, quick,commit)
  - Attachment
    -Prefix (unhappy, postgraduate) or suffix (quickly, commitment)
- Attack program method
  - Tests password against 1000 common passwords (123456, password1,)
  - Combines common passwords with common suffixes (4u , 1)
  - Uses 5000 common dictionary words, 10,000 names, 100,000 comprehensive dictionary words
  - Uses lowercase, initial uppercase, all uppercase, and final character uppercase
  - Makes common substitutions for letters in the dictionary words
    - Examples: $ for s, @ for a

Passwords Defenses

PASSWORD COMPLEXITY

General observations to create strong passwords

- Do not use dictionary words or phonetic words
- Do not use birthdays, family member or pet names, addresses or any personal information
- Do not repeat characters or use sequences
- Do not use short passwords
- Use nonkeyboard characters, or special characters that do not appear on the keyboard

Passwords Defenses

CREDENTIAL MANAGEMENT

Defense against theft of password digest files

- Do not leave a computer running unattended, even if it is in a locked office.
- All screensavers should be set to resume only when a password is entered.
- Do not set a computer to boot from an optical drive or USB flash drive.
- Password-protect the ROM BIOS.
- Physically lock the computer case so that it cannot be opened.

Good password management practices

- Change passwords frequently
- Do not reuse old passwords
- Never write password down
- Use unique passwords for each account
- Set up temporary password for another user's access
- Do not allow computer to automatically sign in to an account
- Do not enter passwords on public access computers
- Never enter a password while connected to an unencrypted wireless network

What You Know: Passwords

PASSWORD SUPPLEMENTS

Problem: managing numerous strong passwords is burdensome for users

Solution: rely on technology to store and manage passwords

Internet Explorer (IE) and Firefox Web browsers contain function that allows user to save passwords

AutoComplete Password in IE
–Encrypted and stored in Windows registry

Disadvantages of password supplements

- Password information specific to one computer
- Passwords vulnerable if another user allowed access to the computer

What You Know: Passwords

PASSWORD MANAGEMENT APPLICATIONS

User creates and stores passwords in single user "vault" file protected by one strong master password

Type	Description	Advantages	Disadvantages
Installed application	Installed as a program on the local computer	Allows the user to access passwords without having to memorize them	It must be installed on each computer used and the vault file must also be updated on every computer used
Portable application	Stand-alone application carried on a USB flash drive	The user is not limited to computers that have the application preinstalled with the vault file	User must always have flash drive present to use the application
Internet storage	Application and/or vault is stored online	Can access program and/or vault from any computer	Storing passwords online may expose them to attacks

Password management applications

What You Have: Tokens and Cards

TOKENS

- Small devices with a window display
- Synched with an authentication server
- Code is generated from an algorithm
- Code changes every 30 to 60 seconds

User **login steps** with a token

- User enters username and code from token
- Authentication server looks up algorithm associated with that user, generates its own code, and compares it to user's code
- If a match, user is authenticated

ADVANTAGES over passwords

–Token code changes frequently

- Attacker would have to crack code within time limit

–User may not know if password has been stolen

–If token is stolen, it becomes obvious

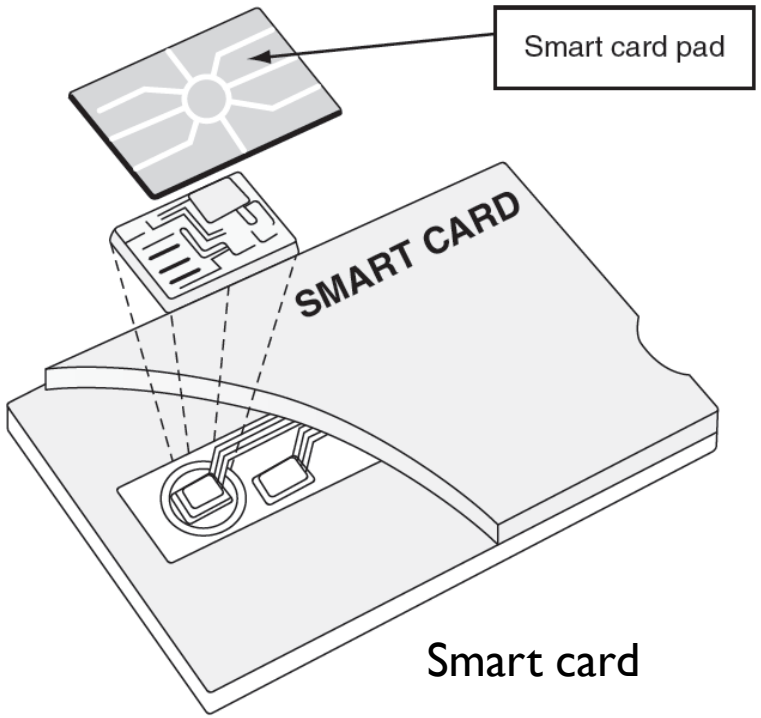
- Steps could be taken to disable account

What You Have: Tokens and Cards

CARDS

- Smart card contains integrated circuit chip that holds information
- Contact pad allows electronic access to chip contents
- Contactless cards

  -Require no physical access to the card



Smart card

What You Are: Biometrics

Standard biometrics

- Uses person's unique physical characteristics for authentication
- Fingerprint scanners most common type
- Face, hand, or eye characteristics also used

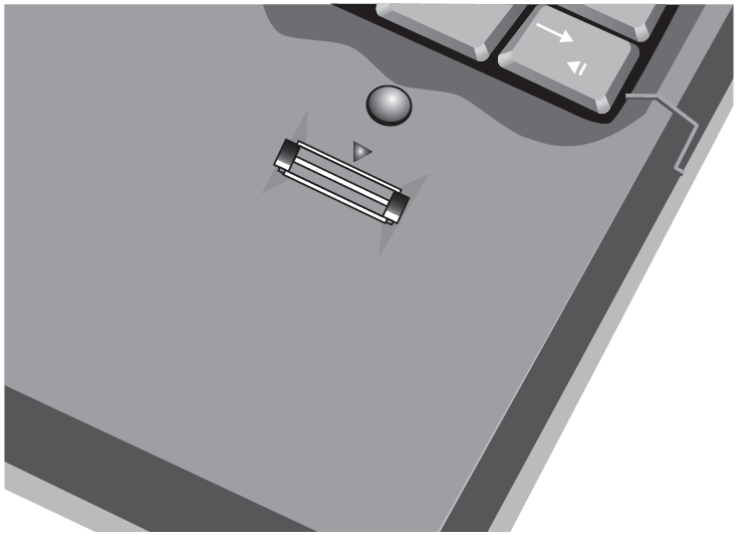
Fingerprint scanner types

Static fingerprint scanner

•Takes picture and compares with image on file

Dynamic fingerprint scanner

•Uses small slit or opening



Dynamic fingerprint scanner

DISADVANTAGES OF STANDARD BIOMETRICS

- Cost of hardware scanning devices
- Readers have some amount of error

-Reject authorized users

-Accept unauthorized users

What You Are: Biometrics

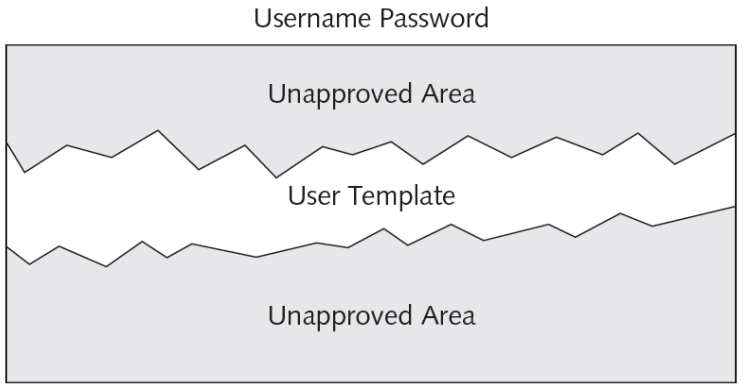
Cognitive biometrics

- Relates to perception, thought process, and understanding of the user
- Easier for user to remember because it is based on user's life experiences
- Difficult for an attacker to imitate
- Example: identifying specific faces
- Example: user selects memorable lifetime events and is asked for details about them
- Predicted to become a key element of authentication in the future

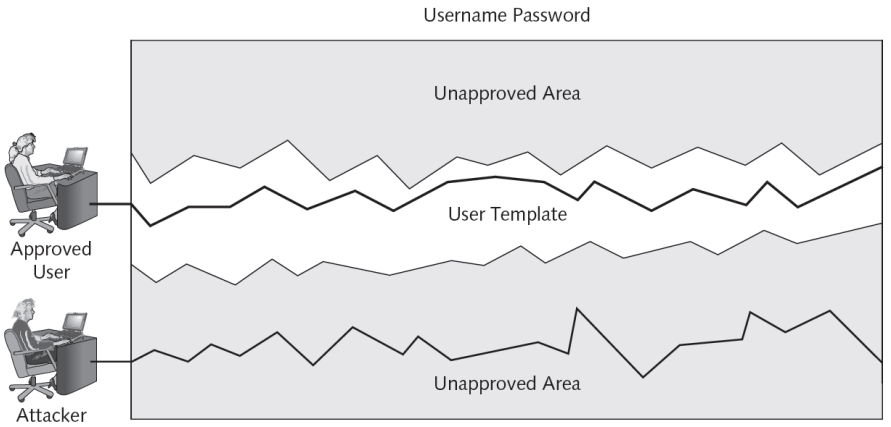
Behavioral Biometrics

Keystroke Dynamics

- Keystroke dynamics
- Attempts to recognize user's typing rhythm
  - •All users type at a different pace
  - •Provides up to 98 percent accuracy
- Uses two unique typing variables
  - •Dwell time (time it takes to press and release a key)
  - •Flight time (time between keystrokes)



Typing template



Authentication by keystroke dynamics

What You Are: Biometrics

Voice recognition

- Several characteristics make each person's voice unique
- Voice template can be created
- Difficult for an attacker to authenticate using a recording of user's voice

Single Sign-On

Identity management

- Using a single authentication credential shared across multiple networks
- Called federated identity management (FIM) when networks are owned by different organizations
- Single sign-on (SSO) holds promise to reduce burden of usernames and passwords to just one

Windows Live ID

- Introduced in 1999 as .NET passport
- Name changed to Microsoft Passport Network, then Windows Live ID
- Designed as an SSO for Web commerce
- Authentication process
  - –User enters username and password
  - –User given time limited "global" cookie stored on computer with encrypted ID tag
- ID tag sent to Web site
- Authentication process (cont'd.)
  - –Web site uses ID tag for authentication
  - –Web site stores encrypted, time-limited "local" cookie on user's computer
- Windows Live ID was not widely supported
- Currently used for authentication on:
  - –Windows Live, Office Live, Xbox Live, MSN, and other Microsoft online services

OpenID

Decentralized open source FIM

•Does not require specific software to be installed on the desktop

•URL-based identity system

•OpenID provides a means to prove a user owns the URL

Authentication process

- User goes to free site and given OpenID account of Me.myopenID.co
- User visits Web commerce or other site and signs in using his Open ID
- Site redirects user to MyOpenID.com where he enters password to authenticate
- MyOpenID.com sends him back to Web site, now authenticated

Security weaknesses

- Relies on DNS which may have own weaknesses
- Not considered strong enough for most banking and e-commerce Web sites

Account Management

- Managing user account passwords
  - –Can be done by setting password rules
  - –Too cumbersome to manage on a user-by-user basis
    - •Security risk if one user setting is overlooked
- Preferred approach: assign privileges by group
  - –Microsoft Windows group password settings
    - •Password Policy Settings
    - •Account Lockout Policy

Attribute	Description	Recommended setting
Enforce password history	Determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24)	24 new passwords
Maximum password age	Determines how many days a password can be used before the user is required to change it; the value of this setting can be between 0 and 999	60 days
Minimum password age	Determines how many days a new password must be kept before the user can change it (from 0 to 999); this setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times, and then change back to their old passwords	1 day
Minimum password length	Determines the minimum number of characters a password can have (0 to 28)	12 characters
Passwords must meet complexity requirements	Determines whether the following are used in creating a password: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters; must contain characters from three of the following four categories: English uppercase characters (A through Z), English lowercase characters (a through z), digits (0 through 9), and nonalphabetic characters (!, $, #, %)	Enabled
Store passwords using reversible encryption	Provides support for applications that use protocols that require knowledge of the user's password for authentication purposes; storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords	Disabled

Password policy settings (Windows group policy)

Attribute	Description	Recommended setting	Comments
Account lockout duration	Determines the length of time a locked account remains unavailable before a user can try to log on again (a value of *0* sets account to remain locked out until an administrator manually unlocks it)	15 minutes	Setting this attribute too high may increase help desk calls from users who unintentionally locked themselves out
Account lockout threshold	Determines the number of failed login attempts before a lockout occurs	30 invalid attempts	Setting this attribute too low may result in attackers using the lockout state as a denial of service (DoS) attack by triggering a lockout on a large number of accounts
Reset account lockout counter after	Determines the length of time before the account lockout threshold setting resets to zero	15 minutes	This reset time must be less than or equal to the value for the account lockout duration setting

Account lockout policy settings (Windows Active Directory)

Trusted Operating Systems

Operating System Basic Flaws

- Size: millions of lines of code make vulnerabilities difficult to recognize
- One compromised application can impact entire computer
- Applications cannot authenticate themselves to each other
- No trusted path between users and applications
- Operating systems do not use principle of least privilege

Trusted Operating Systems

- OS designed to be secure from the ground up
- Can keep attackers from accessing critical parts of the system
- Can prevent administrators from inadvertently making harmful changes

Vendors developing trusted OSs
Focusing on securing OS components and other platform elements

One approach: compartmentalize services within trusted OS for individual customers

Summary

Authentication credentials can be classified into three categories: what you know, what you have, and what you are

- Passwords provide a weak degree of protection
  - Must rely on human memory
- Most password attacks today use offline cracking
  - Attackers steal encrypted password file
- A token is a small device that generates a code from an algorithm once every 30 to 60 seconds

Biometrics bases authentication on characteristics of an individual

- Standard, behavioral, and cognitive biometrics

- Single sign-on allows a single username and password to gain access to all accounts
- Group Policy settings allow an administrator to set password restrictions for an entire group at once
- Trusted operating systems are designed for security from the ground up