Gartner research director John Pescatore states:

Businesses face increased threats from hackers using keystroke loggers to grab user names and passwords at Internet cafes and wireless hotspots in airports and hotels, and the user-name-password approach isn’t effective enough to protect business systems, applications, and data.

"It's an increasing problem, and corporations need to do something about it."

**Learning Objectives**

- Describe an IS framework that incorporates the five main security goals
- Explain how access controls are used to support these five main security goals
- Describe the standard access controls that most organisations adopt
- Discuss weaknesses and limitations of some of these standard access controls
**Effective Security Goals**

- **AUTHENTICATION**
  - Verify identity of users
  - Only authorised users to access appropriate resources
- **AVAILABILITY**
  - Ensure system is available for use at all times
- **CONFIDENTIALITY**
  - Ensure confidentiality of communication among authorised parties
- **DATA INTEGRITY**
  - Ensure data communications, files and programs are not tampered with
- **NON-REPUDIATION**
  - To provide undeniable proof that a certain user sent a certain message and to prevent the receiver from claiming that a different message was received

**Security Goals**

- **AUTHENTICATION**
  - Verify identity of users
  - Only authorised users to access appropriate resources
- **AVAILABILITY**
  - Ensure system is available for use at all times
- **CONFIDENTIALITY**
  - Ensure confidentiality of communication among authorised parties
- **DATA INTEGRITY**
  - Ensure data communications, files and programs are not tampered with
- **NON-REPUDIATION**
  - To provide undeniable proof that a certain user sent a certain message and to prevent the receiver from claiming that a different message was received

**Risk Management framework**

- This model provides a framework within which to secure an organisation’s assets
- It supports the security of an information system
- Each part of the framework builds on the next part
- Feedback loops support each part of the framework
Step 1: Risk Assessment

- Involves making decisions about how to deal with each perceived threat
  - Ignore threat (risk acceptance)
- Identify critical assets
- Identify vulnerabilities that may be impacted by a perceived threat

What methods do we use to do this?

Step 2 – Risk Mitigation

- Use the outcome of the risk assessment to identify the optimum set of mitigation (control) measures

Authentication Defined

- Authentic
  - Conforming to fact and therefore worthy of trust, reliance, or belief
  - Having a claimed and verifiable origin or authorship; not counterfeit or copied
- Authenticate
  - To establish the authenticity of; prove genuine
- Authentication
  - The verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter or a cheque
Authentication techniques

- Identification plus verification
- Purpose: verify user ID is authorised
- Variety of techniques
  - Forces the party to produce proof of identity
    - Something they know eg password
    - Something they have eg a metal key
    - Something they are eg fingerprint
  - NB: These are in increasing order of difficulty for a masquerader to provide
  - Biometrics
  - Smartcards
  - User id/Password Pairs

Authentication Techniques

- Single sign on
  - Passwords
  - Encryption techniques
- Tokens
- Biometrics
- All of the above??

Single Sign On

- Provides single-step access to all target platforms and applications via a single, consistent login interface (portal)
- Identity management system
  - An Identity Management system enables and maintains user access to network resources. Includes:
    - the creation of the user entity
    - authorisation and permissions.
  - SSO delivers password management functionality, providing an additional layer of control and security to a comprehensive Identity Management system.

ROI implementing Single Sign on

Why Have Single Sign On

- simplify sign-on for end users,
- reduce helpdesk support cost for password resets,
- improve security through multi-factor authentication platform
  - smart cards
  - fingerprint biometrics
  - hardware tokens
  - passwords, and/or a combination of these
- digital identity management


Passwords

- Most common and easiest form of access
- To be effective:
  - Requires the use of a secure channel through the network to transmit the encrypted password
- Not very secure
- WHY USE THEM??

Authentication process

Attacks and defences evolve in response to each other. As attacks develop, defences develop in response to newer attacks evolve to circumvent the new defences.
Passwords (Pros)

- User friendly
  - People get the concept (like an ATM pin #)
- Two factor authentication
  - Combine passwords with a (smart card) token
  - ATM card and PIN – improved protection
- Easy to manage
- Supported across IT platforms

Password Security Management

- Log accesses
- Validation programs
- Other techniques
  - Enforce Password changes = 30 days?
  - Audit logs
  - Privacy policy

Password Security Controls

- Require a minimum password length
  - “Wider is better”
- Require non-alphanumeric text
  - Increases your password alphabet
  - Passwords more difficult to crack
- Attempt to crack passwords
  - During password change
- Maintain a password history
  - Attempts to regulate password reuse
  - Easily circumventable
  - Creates a list of users passwords (bad)

Password Security controls

- Develop a password expiration policy
  - Passwords expire at regular intervals
- Never store a password as plain text
  - One-way crypt algorithms for password files
  - Symmetric ciphers for scripts
- Maintain audit logs
  - Useful in tracking violators
  - Privacy issues
- Policy for lost passwords
- Policy for password cancellation
  - HR
  - When staff member leaves
  - When staff member changes job role
There is a **direct relationship** between the ease with which a password can be remembered and the ease with which it can be guessed.

Without a gimmick, a password that is difficult for an unauthorized person to guess is usually difficult for a user to remember.

If a password is easy to remember, it is probably easy for someone else to guess.

---

A 2002 Pentasafe Security Technologies survey of 15,000 staff members in 600 organisations in the US and Europe found:

- 25% use common dictionary terms eg banana
- 50% use names of family members, pets etc
- 30% use names of pop idols or sport heroes
- 10% use fantasy names
- 10% use complex passwords - difficult to break

---

Users choose easy to guess passwords

Determined by experimentation

Share passwords

Difficult to make users more vigilant – often forget passwords

Vulnerable to hacker attacks

---

*Given the speed of computers that can crack passwords, long passwords are needed for safety*

Two character passwords = 676 possibilities

Four character passwords = 400,000 possibilities

Six character passwords = 300 million possibilities
Lost Password - Social Engineering Attacks

- An attacker contacts the ‘help desk’ claiming to be the owner of an account and requests a password reset.
- The help desk employee under pressure may reset the account password.
- The attacker then effectively owns the account and the original owner is now locked out.

A QUARTER TO A THIRD OF ALL HELP DESK CALLS ARE DUE TO LOST PASSWORDS (Panko, 2004)

Countering These Attacks

- What can you do?
- The staff member must come to the IT help desk and sign in for the new password and show some form of ID.
- Automate password resets through the system.

Shoulder Surfing

WATCHING SOMEONE WHILE THEY KEY IN A PASSWORD
- To slow the keying in of the password, the attacker may talk to the person.
- A few characters in sequence may be all it takes for access (Panko, 2004)

Tokens “something the user has”

- Plastic cards (e.g., magnetic stripe cards, smart cards, keys, badges

SafeWord Gold 3000
"authenticator" or a "token"

- A device used to generate dynamic passwords while logging onto a network.
- Token types range from software tokens (that may reside on PCs, PDAs, cellular phones, smart cards, etc.) to
- hardware tokens that resemble small hand-held calculators.

Advantages

- Token must be stolen or misplaced to lose the control
- User is aware of any theft or loss
- User accepts responsibility for token
- Can't be shared simultaneously with another person
- Possession by unauthorised person can sometimes be proven

Disadvantages

- FORGERY/THEFT

Plus/Minus!!

Plastic Cards

- In common use ATM/EFTPOS
- Magnetic strip with user ID data encoded
- Magnetic strip info and PIN transmitted to computer – two factor authentication
- PIN encryption may occur prior to transmission

Advantages:

- Well accepted by the public
- Cheap
- Convenient

Disadvantages:

-Forgery
- Theft
- Damage

Plastic Card – Tighter Controls

- Embossing with user ID
- Holographic images
- Encrypted magnetic strip information
- Change PIN if requested (e.g. on theft)
Biometric Authentication

'Something the user has'

- Individual must be physically present
- Provide attributes physically
  - Fingerprint
  - Voice recognition
  - Iris recognition
  - Face recognition
  - Hand geometry
  - Signature recognition
    - http://www.cybersign.com/

Most common - relatively inexpensive to implement

New Methods

- Breath testing – DNA
- Gait recognition (what is this??)

Broader Use Of Biometrics

- Face matching surveillance technology
  - Super Bowl at Raymond James Stadium, Tampa Florida, 2001
  - Soccer hooligans
- Iris and fingerprint scans
  - In use/tests currently at major US airports
- Combinations of several methods will reduce the vulnerability to replay attacks
  - Minimise false positives
  - Small amount of false negatives

Biometric Enrollment

Each user must first be enrolled in the system.

1. Each person’s biometric data must be scanned by an ‘Information Reader’
2. Processed to extract a few key features
   - In fingerprints (there are 18 key points – police records)
3. Stored as the user’s template in the database


Goodness of fit - MATCH INDEX

- A match index is computed to determine the goodness of fit
- If the match index meets DECISION CRITERIA the person is verified to be who they say they are according to the system

Plus/minus

ADVANTAGES
- Unique to an individual – relatively difficult to copy
- No need to remember a password or carry a token

DISADVANTAGES
- Can be costly
- Injury
- Compromised central data storage (e.g. signature)
- Suitable for organisations with highly sensitive data

Biometric Identification

- The applicant does not claim to be a particular person
- The system must identify the applicant
  - To determine who he or she is
- The applicant’s biometric sample data must be matched against the data against EVERYONE WHOSE PROFILE IS STORED IN THE SYSTEM
- The system makes the access decision based on the most probable acceptable goodness of fit (match)
Biometric Authenticator

<table>
<thead>
<tr>
<th>Key</th>
<th>The key advantage of biometric measurement of the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages of using a biometric authenticator:</td>
<td>Greater security than simple biometric passwords.</td>
</tr>
<tr>
<td></td>
<td>Provides protection against identity theft.</td>
</tr>
<tr>
<td>Disadvantages:</td>
<td>High risk of false positives</td>
</tr>
<tr>
<td></td>
<td>False identification leads to false acceptance.</td>
</tr>
<tr>
<td></td>
<td>Acceptance when should reject.</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
</tr>
<tr>
<td>GOOD</td>
<td>Reject when should accept</td>
</tr>
<tr>
<td>BAD</td>
<td>Accept when should reject</td>
</tr>
</tbody>
</table>

False rejection/false acceptance

Airport Security Systems

- Face identification to catch criminals
- A tiny false positive rate will mark dozens of innocent people
- Can Face scanners be easily fooled?

Can Face scanners be easily fooled?

- 8-week trial of face detection system at Palm Beach International Airport
- The system was loaded with data on a small number of volunteers
- 455 out of 958 volunteers were recognised
- A false reject rate of more than 50%
- Further the recognition rate when down when:
  - The person wore glasses worse if tinted lenses
  - The person looked away from the camera
Inherent Problems?

- Size of the database
- The clarity of the photos fed into the system
  - Poor photos would reduce the detection rate
  - Many terrorists have only been identified by their photos (see handout)
- Fingerprint and Iris sensors can be fooled
  - Breathing on them
  - Placing a small bag of water on the sensor
  - Biometric signature being stolen from the database

Authentication Factors

<table>
<thead>
<tr>
<th>Factor</th>
<th>Benefits</th>
<th>Weaknesses</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Something you know, password</td>
<td>Easy to remember, cost effective</td>
<td>Hard to remember, cost of handling forgotten passwords</td>
<td>Password, PIN, biometric tokens</td>
</tr>
<tr>
<td>Something you have taken</td>
<td>Easy to collect, cost of collecting</td>
<td>Easy to steal, cost of handling stolen tokens</td>
<td>Credit card, Social Security ID</td>
</tr>
<tr>
<td>Something you are biometric</td>
<td>Easy to collect, cost of collecting</td>
<td>Easy to steal, cost of handling stolen tokens</td>
<td>Fingerprint, Iris fingerprint</td>
</tr>
</tbody>
</table>

Access Controls

- Users only have access to appropriate resources
- Determined by security policy administrator
- Implemented via hardware, devices and/or software (OS, IS)

Access control Principles

- Minimal privilege/exposure
- Regular monitoring of access privileges
- Limit accesses to only those resources required by user for tasks ("need to know")
- Physical, logical and integrated access control
- Monitor logs
A Word About Cost
(Secure Computing Whitepaper, 2002)

- The cost of authentication systems meeting the requirements of generally accepted computing practices is significant.
- Requires careful consideration during the selection and implementation stages, and requires careful management when they are used.
- Costs are associated with acquisition, installation, customization, administration, user training, productivity impact, and maintenance of such systems.
- Planners should ask vendors for detailed statements, policies, and prices for each of these factors, and that planners determine the real cost of these systems rather than concentrate on one or two areas.

Conclusion

A large proportion of breaches occur within the organization’s system therefore secure access controls are a major part of an organization’s security arsenal.

Security management policies and procedures are an important component to support the variety of standard access controls.

Conclusion cont’d

Today, the right authentication choices for a particular Enterprise or application depend on how people use the systems in question, how the systems are built, and what types of attacks they expect.

The authentication capabilities of today’s commercial systems, and the promise of tomorrow’s evolving systems, all stand upon past successes and failures.

Review Questions

- To establish an effective security framework five main security goals must be supported.
  - Discuss the appropriate access controls which would support these goals.
References – additional readings

- Smith, R. E. Authentication: From Passwords to Public Keys (Chapter 1) Publisher: Addison-Wesley

Appendix

- Choosing strong passwords

Choosing Strong Passwords:

- That is at least eight characters long.
- That contains uppercase and lowercase letters.
- That contains at least one number or special character.
- That is not a dictionary word in any language, slang, or jargon.
- That cannot be easily guessed and is easy to remember.

Remember to change your password every 30-60 days.

Strong Passwords (examples):

- Wwe&nadtd
- IsfgaWDo6
- Md#1imh
- tmW2rpw
- 2BoN2bTist?
- 3bmsftw1491
- S2eobbwttfcd
- mkrG8bs$