

Secure Operating systems

by Dr. Hesham Abou Elfetouh

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

مزيد من التفاصيل



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 6

In Previous Lecture you learned:

- What is “Program security”
- Basic approaches to having secure programs
- Controls for Security
- Developmental Controls for Security
- Administrative Controls for Security
- Operating System Controls for Security



This chapter covers the following topics and concepts:

User authentication

Password authentication

Probable Passwords

Passwords Likely for a User

Password Selection Criteria

One-Time Passwords

Salt



When you complete this chapter, you will be able to:

- Know What is the “User authentication”
- Explain the Password Authentication
- Illustrate the Implementation of Access Control
- Know the Passwords Likely for a User



User authentication

- “The process of verifying an identity claimed by or for a system entity.”
- driver's license
- passports
- voice recognition
- fingerprint
- retina matching





Password Storage

Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm\$oto!4

Plaintext

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Concealed



Password Authentication

- The most common authentication mechanism for user to operating system is a **password**.
- A "word" known to computer and user.
- widely used line of defense against intruders
 - user provides name/login and password to the security system (**identification step**)
 - system compares password with the one stored for that specified login (**verification step**)
- the user ID:
 - determines that the user is authorized to access the sys
 - determines the user's privileges
 - is used in access control





Authentication Methods

the four means of authenticating user identity are based on:

**something
the individual
knows**

- password, PIN, answers to prearranged questions

**something
the individual
possesses
(token)**

- smartcard, electronic keycard, physical key

**something
the individual
is (static
biometrics)**

- fingerprint, retina, face

**something
the individual
does
(dynamic
biometrics)**

- voice pattern, handwriting, typing rhythm





Authentication mechanisms

- Two or more forms can be combined for more solid authentication.
- a bank card and a PIN combine something the user has with something the user knows.



Why Passwords?

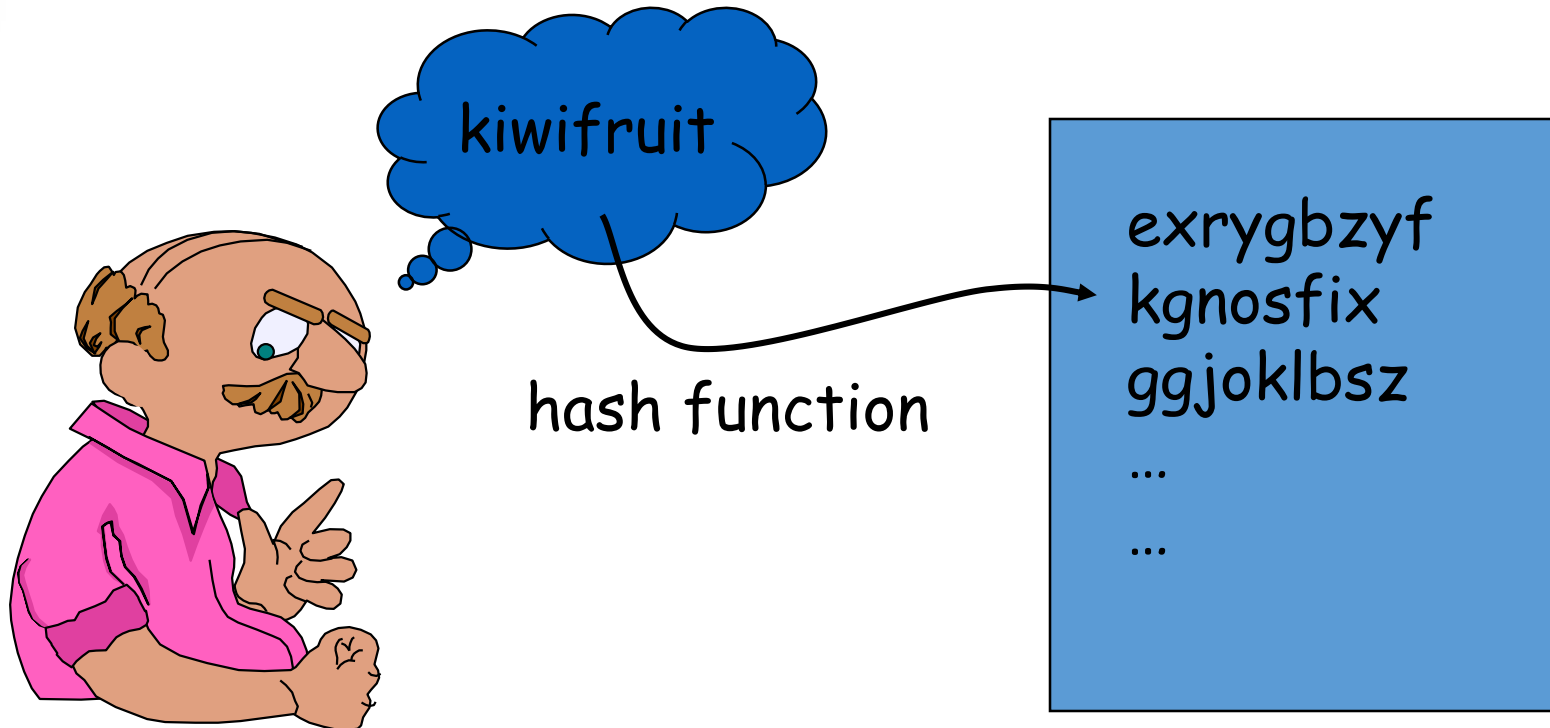
- Why is “something you know” more popular than “something you have” and “something you are”?
- **Cost**: passwords are free
- **Convenience**: easier for System Administrator to reset pwd than to issue user a new thumb



Basic password scheme

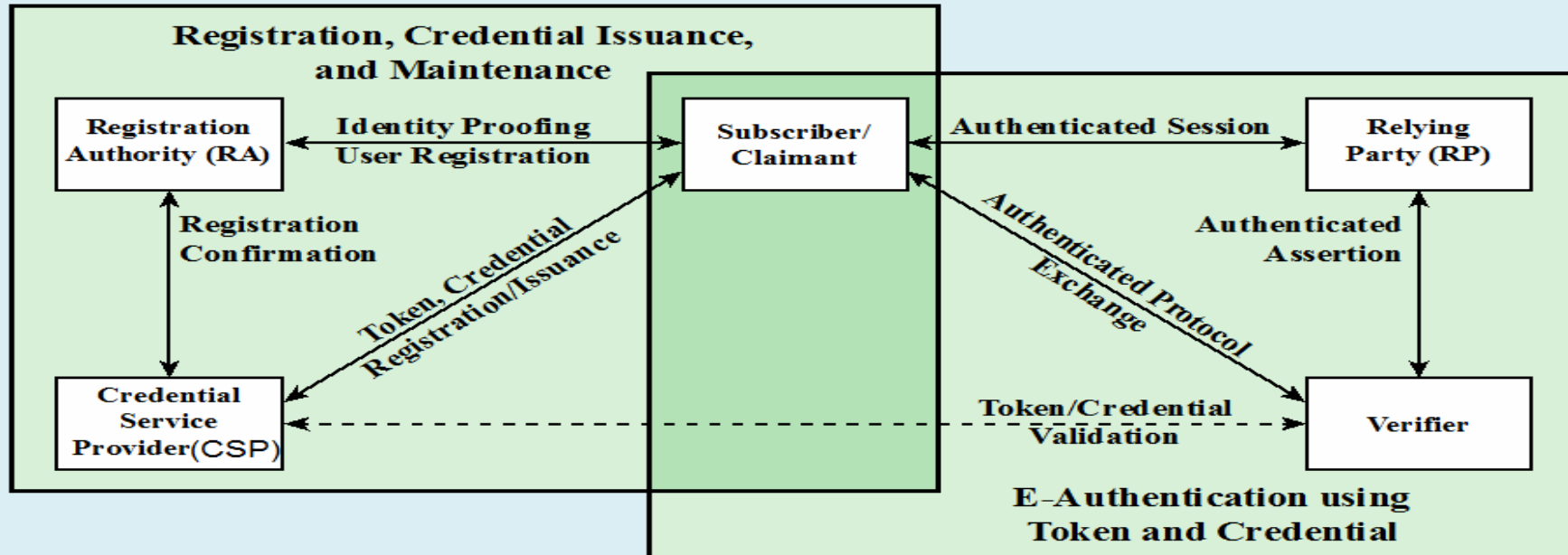
User

Password file





Authentication model



Authentication Architectural Model



Keys Versus Passwords

- If a password is 8 characters long (8 bytes) with 256 possible choices for each character → 256^8 possible passwords.
 - E.g. password
- If a key with 64-bit (8 bytes) cryptographic key → 2^{64} possible keys. (Trudy must try 2^{63} keys before she expects to find the correct one)
 - E.g. Kf&Yw!a[
- Although $2^{64} = 256^8$ (8 bytes), and this appears to be equivalent, users don't select passwords at random because users must remember their passwords.



Basic password scheme

- Hash function $h : \text{strings} \rightarrow \text{strings}$
 - Given $h(\text{password})$, hard to find password
 - No known algorithm better than trial and error
- User password stored as $h(\text{password})$
- When user enters password
 - System computes $h(\text{password})$
 - Compares with entry in password file
- No passwords stored on disk



Passwords difficulties

- Loss
 - if the user loses the password, a new one must be assigned.
- Use
 - Supplying a password for each access to a file can be inconvenient and time consuming.
- Disclosure
 - If a password is disclosed to an unauthorized individual, the file becomes immediately accessible.
 - If the user changes the password, all the other users must be informed of the new password because their old password will fail.
- Revocation
 - To revoke one user's access right to a file, someone must change the password, thereby causing the same problems as disclosure.



Password Vulnerabilities

**offline
dictionary
attack**

**popular
password attack**

**workstation
hijacking**

**exploiting
multiple
password use**

**specific account
attack**

**password
guessing against
single user**

**exploiting user
mistakes**

**electronic
monitoring**





Countermeasures

- controls to prevent unauthorized access to password file
- intrusion detection measures
- rapid reissuance of compromised passwords
- account lockout mechanisms
- policies to inhibit users from selecting common passwords
- training in and enforcement of password policies
- automatic workstation logout
- policies against similar passwords on network devices



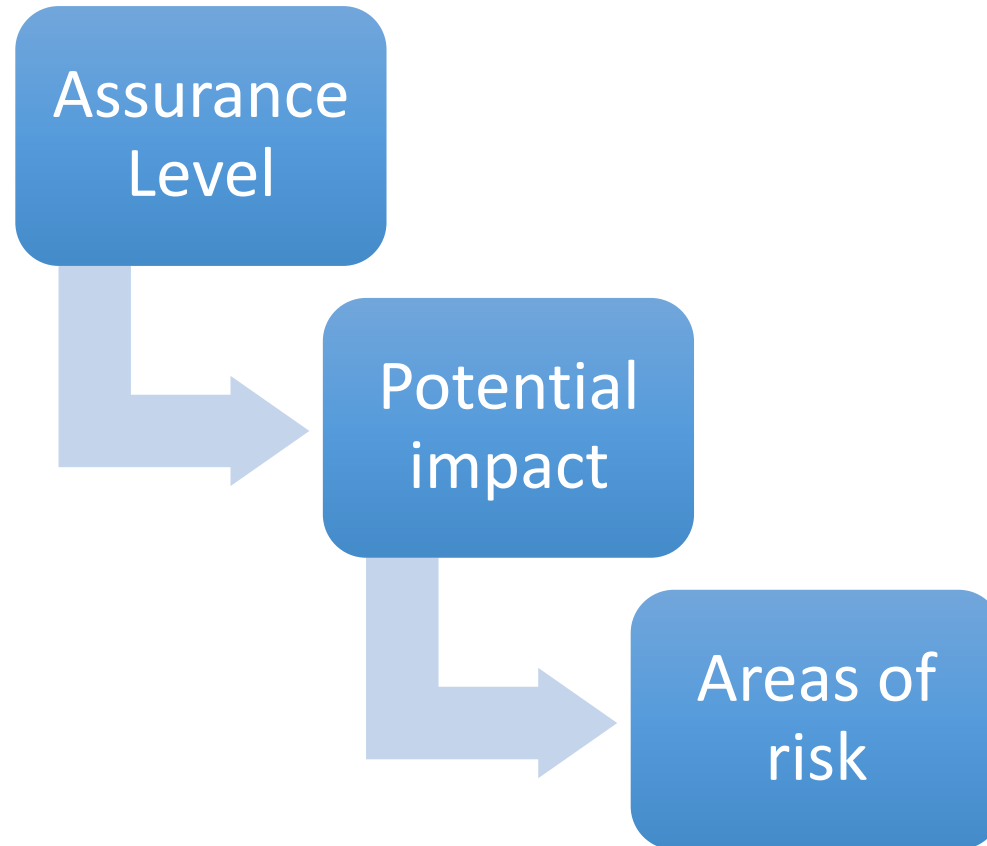
Additional Authentication Information

- Limiting users to certain workstations or certain times of access.
- Using additional authentication information is called **multifactor authentication**
- Two forms of authentication (which is, not surprisingly, known as **two-factor authentication**) are better than one,



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 used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1

- Little or no confidence in the asserted identity's validity

Level 2

- Some confidence in the asserted identity's validity

Level 3

- High confidence in the asserted identity's validity

Level 4

- Very high confidence in the asserted identity's validity





Potential Impact

- There are 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

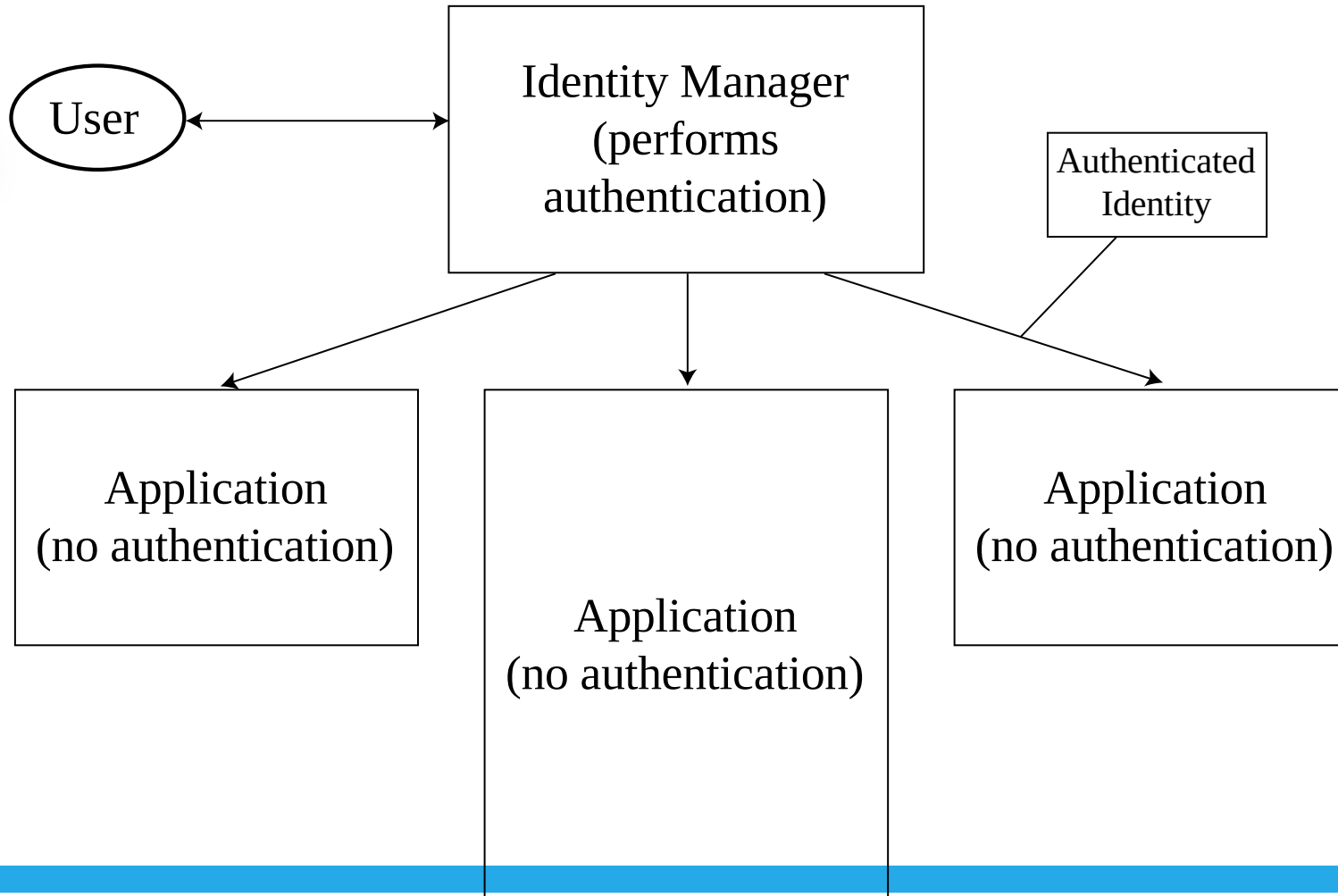


Access Control

- Two parts to access control
- **Authentication:** Are you who you say you are?
 - Determine whether access is allowed
 - Authenticate human to machine
 - Or authenticate machine to machine
- **Authorization:** Are you allowed to do that?
 - Once you have access, what can you do?
 - Enforces limits on actions
- Note: “access control” often used as synonym for authorization

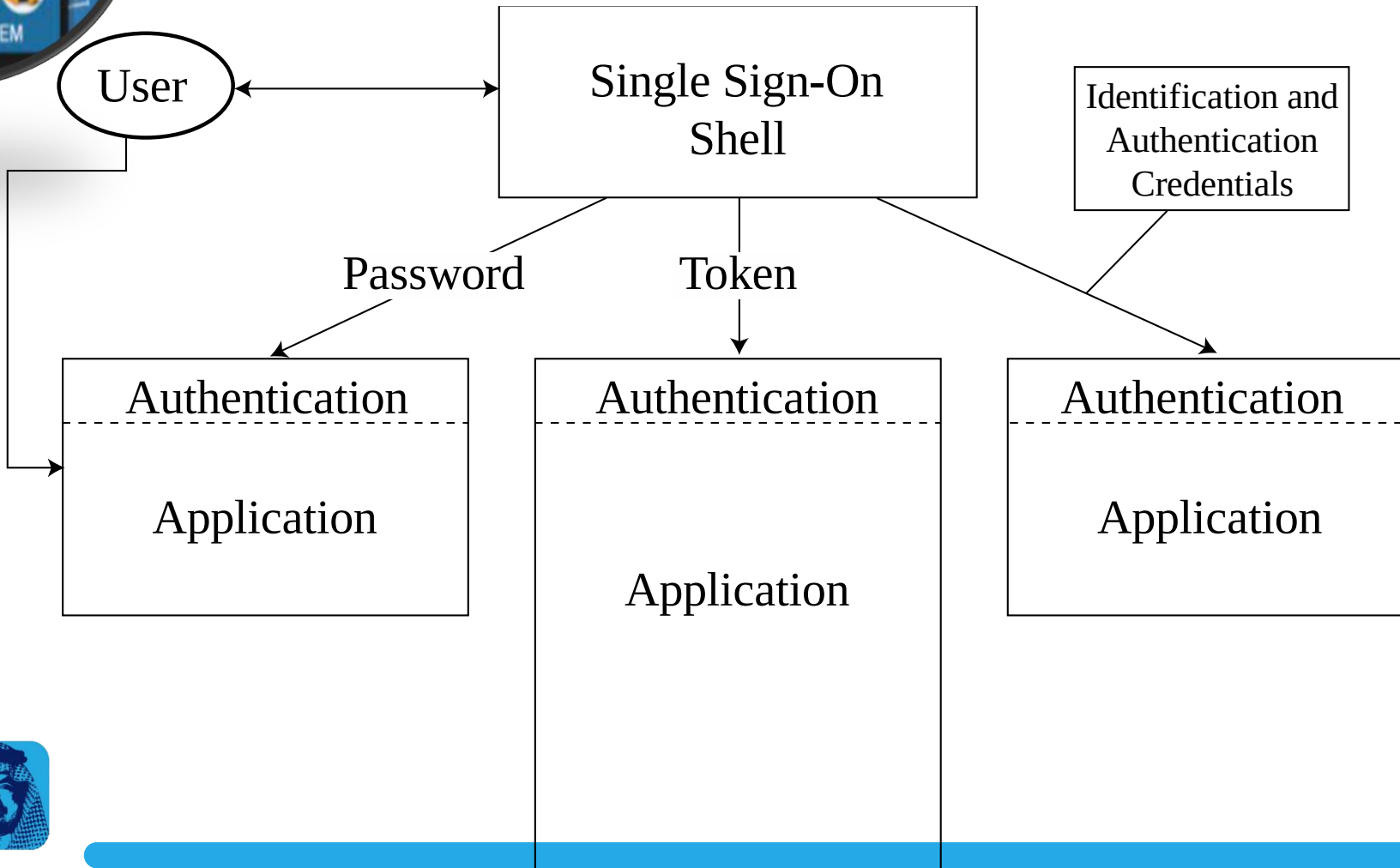


Federated Identity Management





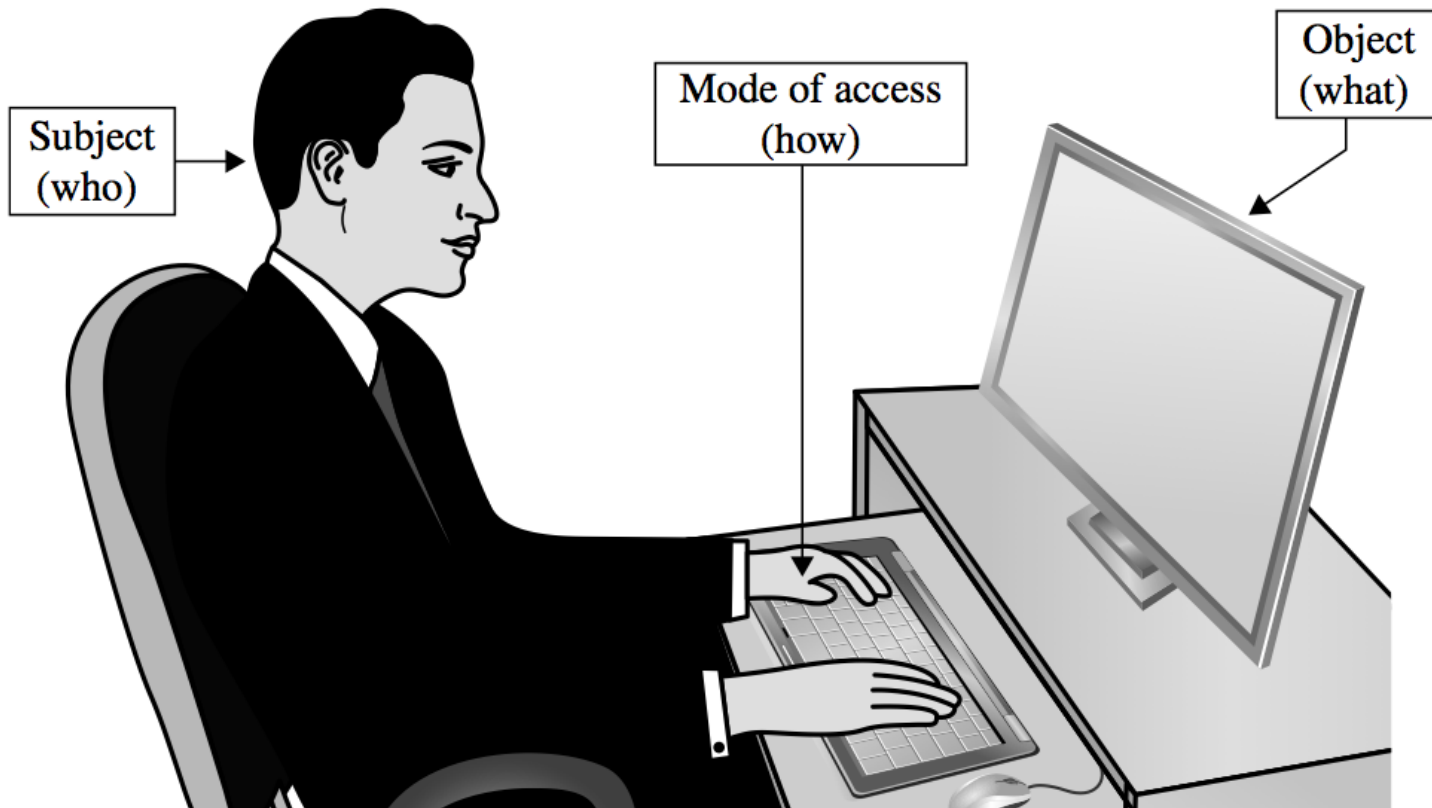
Single Sign-On





Access Control

Policy:
Who + What + How = Yes/No





Access Policies

- Goals:
 - Check every access
 - Enforce least privilege
 - Verify acceptable usage
- Track users' access
- Enforce at appropriate granularity
- Use audit logging to track accesses

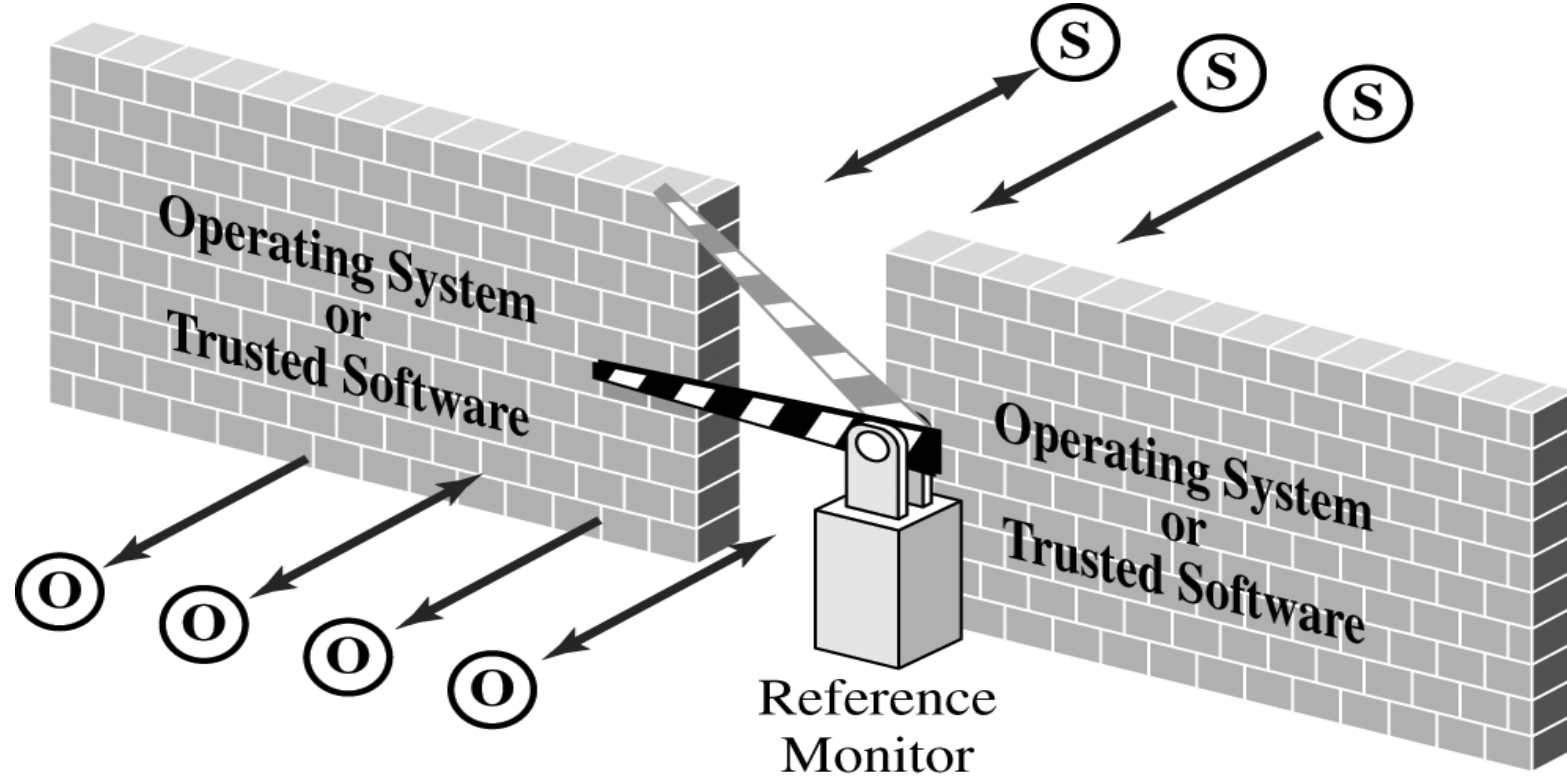


Implementing Access Control

- Reference monitor
- Access control directory
- Access control matrix
- Access control list
- Privilege list
- Capability
- Procedure-oriented access control
- Role-based access control

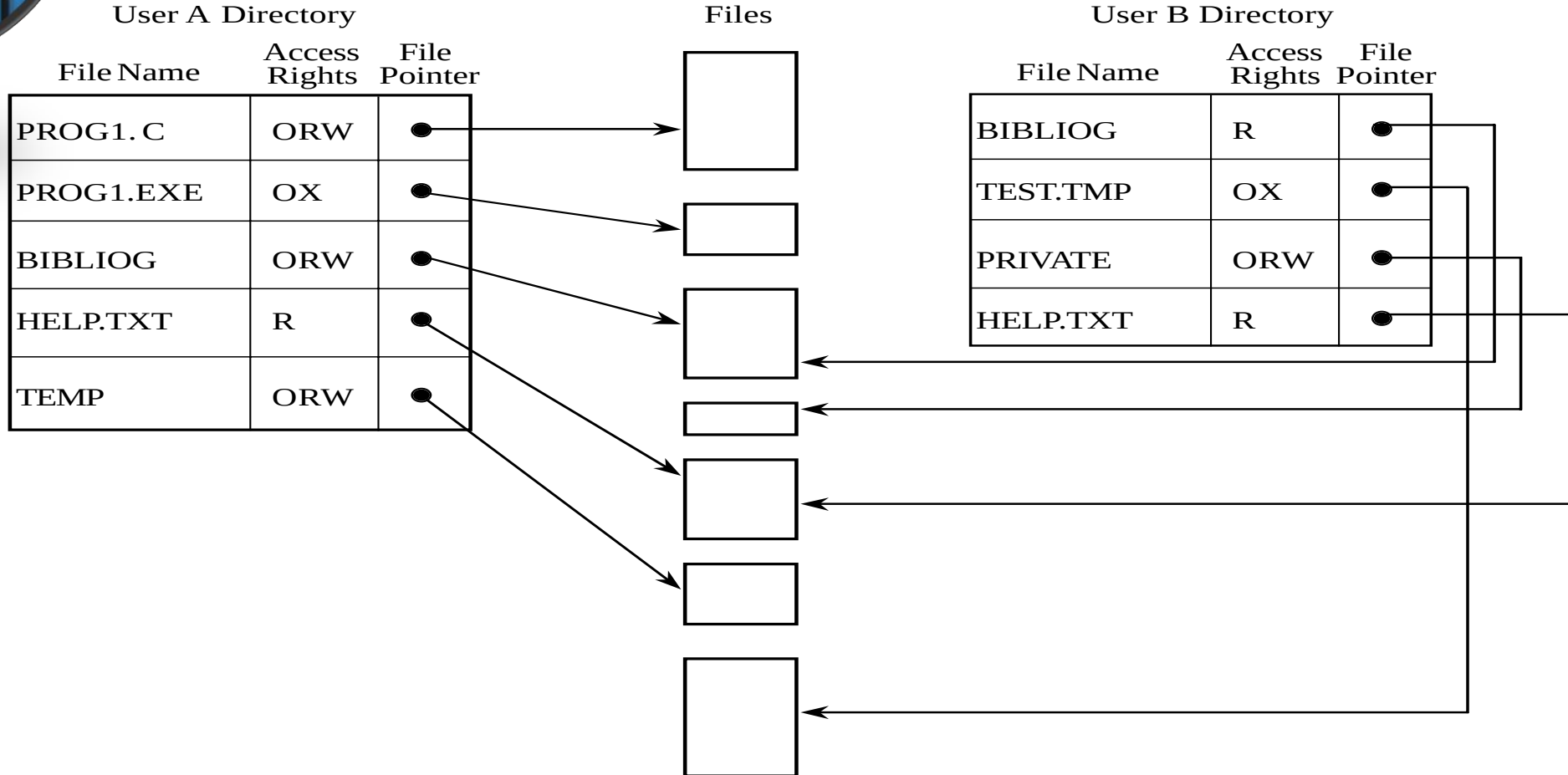


Reference Monitor





Access Control Directory



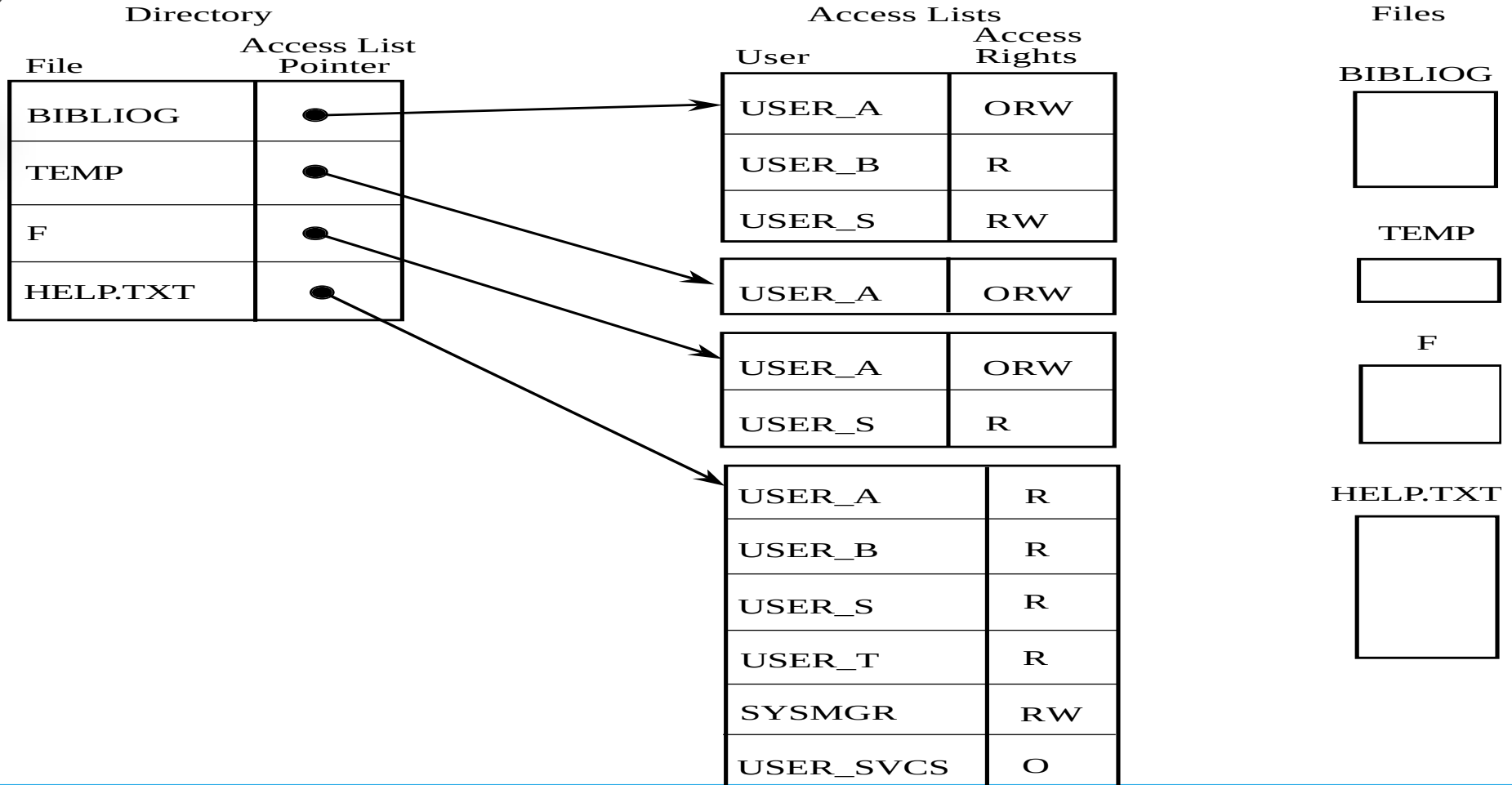


Access Control Matrix

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W



Access Control List





Probable Passwords

Think of a word



Probable Passwords (count)

- Is the word you thought of long?
 - Is it uncommon?
 - Is it hard to spell or to pronounce?
- The answer to all three of these questions is probably **no**.



Probable Passwords (count)

- If people prefer short passwords to long ones, the penetrator will plan to try all passwords but to try them in order by length.
- There are only $26^1 + 26^2 + 26^3 = 18,278$ passwords of length 3 or less.
- At the assumed rate of one password per millisecond, all of these passwords can be checked in 18.278 seconds,



Probable Passwords (count)

- the trials to 4 or 5 characters raise the count only to 475 seconds (about 8 minutes) or 12,356 seconds (about 3.5 hours), respectively.
- People tend to choose names or words they can remember
- Many computing systems have spelling checkers that can be used to check for spelling errors and typographic mistakes in documents.
- Trying all of these words as passwords takes only 80 seconds.



Passwords Likely for a User

- People typically choose personal passwords, such as the name of a spouse, a child, a brother or sister, a pet, a street name, or something memorable or familiar.
- If we restrict our password attempts to just names of people (first names), streets, projects, and so forth, we generate a list of only a few hundred possibilities at most.



Passwords Likely for a User (count)

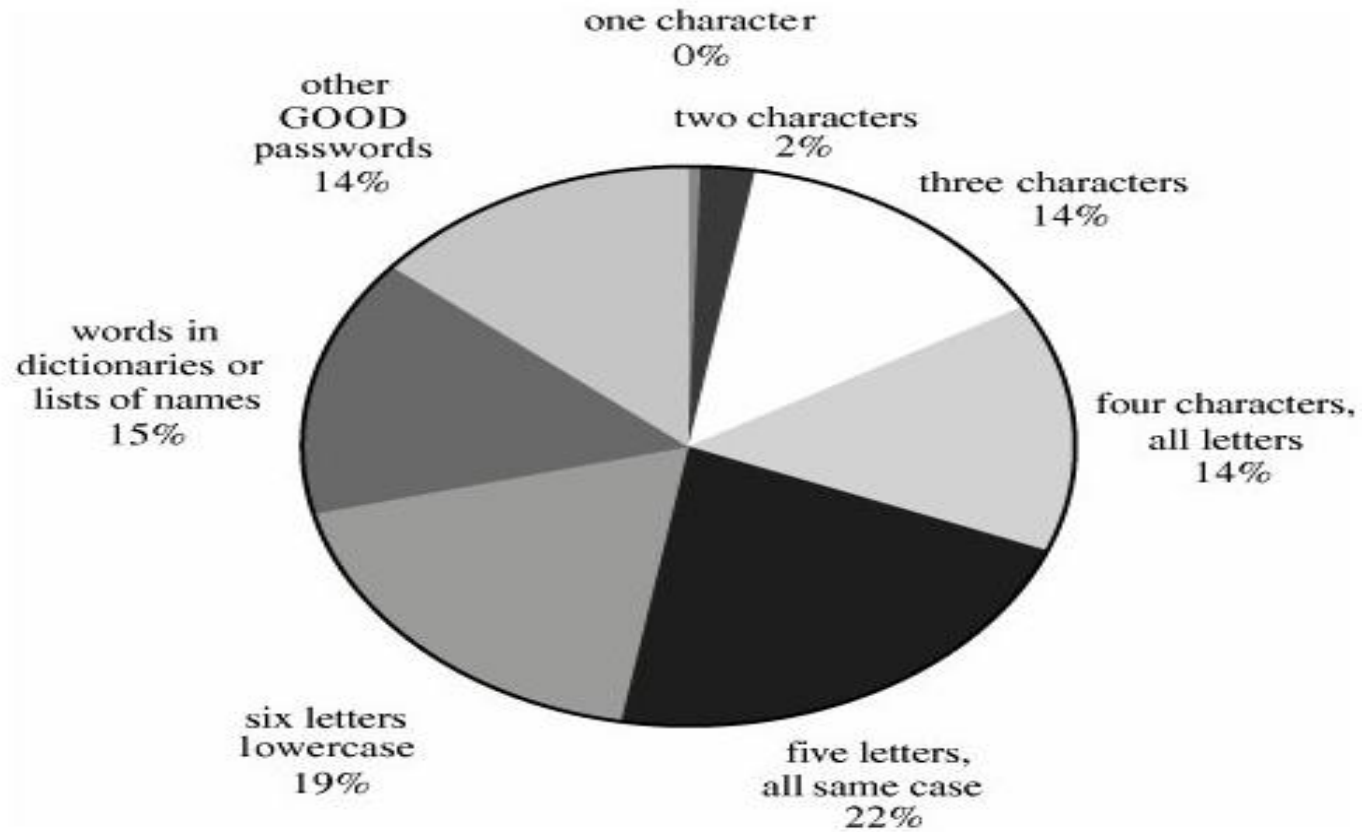
Distribution of Actual Passwords.

15	0.5%	were a single(!) ASCII character
72	2%	were two ASCII characters
464	14%	were three ASCII characters
477	14%	were four alphabetic letters
706	21%	were five alphabetic letters, all the same case
605	18%	were six lowercase alphabetic letters
492	15%	were words in dictionaries or lists of names
2831	86%	total of all above categories



Passwords Likely for a User (count)

Users' Password Choices.





Passwords Likely for a User (count)

- The British online bank Egg found users still choosing weak passwords :
 - A full 50 percent of passwords for their online banking service were family members' names
 - 23 percent children's names
 - 19 percent a spouse or partner
 - 9 percent their own



www.phenoelit.de/dpl/dpl.html

Default Password List

Last updated: 02.22.2010

Vendor	Model	Version	Access Type	Username	Password	Privileges	Notes
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet		
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech		
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)		
3COM	LANplex	2500	Telnet	debug	synnet		
3COM	LANplex	2500	Telnet	tech	tech		
3COM	LinkSwitch	2000/2700	Telnet	tech	tech		
Huawei	E960			admin	admin	Admin	
3COM	NetBuilder		SNMP		LMI	snmp-read	
3COM	Netbuilder		Multi	admin	(none)	Admin	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin	
3COM	SuperStack II Switch	2200	Telnet	debug	synnet		
3COM	SuperStack II Switch	2700	Telnet	tech	tech		
3COM	OfficeConnect 812 ADSL		Multi	admin	admin	Admin	
3COM	Wireless AP	ANY	Multi	admin	comcomcom	Admin	Works o
3COM	CellPlex	7000	Telnet	tech	tech	User	
3COM	cellplex	7000	Telnet	admin	admin	Admin	
3COM	cellplex	7000		operator	(none)	Admin	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin	
3COM	3Com SuperStack 3 Switch 3300XM			security	security	Admin	
3COM	superstack II	1100/3300		3comcso	RIP000	initialize	resets a
3COM	LANplex	2500	Telnet	tech	(none)	Admin	



جامعة القادسية
EVERYONE'S SMART UNIVERSITY



geodsoft.com/howto/password/common.htm



GeodSoft

Good and Bad Passwords How-To

An Example List of Common and Bad Passwords

I have removed the long list of common passwords due to excessive traffic levels, and may restore it sometime after they return to normal. I wish I had never created this list, even though it has become by far the most popular page on this site. All such lists are intellectually dishonest, regardless of how accurate they may be, or how carefully they were prepared. Most people who do not find their password in such a list develop a false sense of security. The simple fact is that any competent cracker will be working from a list many times larger than the largest common password list, and the cracker's list will include virtually every word in any common password list. If your password can be found in any dictionary or online "word" list, where words include such character sequences as "qwerty", "abcd1234", or "thx1138", you have a password just as bad as those listed in common password lists. If you have made any unusual transformations (such as described in [Guiding Text](#)...

[Home](#) >
[How-To](#) >
[Good Passwords](#) >
[common.htm](#)

<[P Windows Weaknesses](#)
[N Password Footnotes](#)

[What's New](#)
[How-To](#)
[Opinion](#)
[Book](#)

[Email address](#)

Site map:
[Home](#)
[What's New](#)
[About GeodSoft](#)
- [Large Web Project](#)
- [Designing GeodSoft](#)



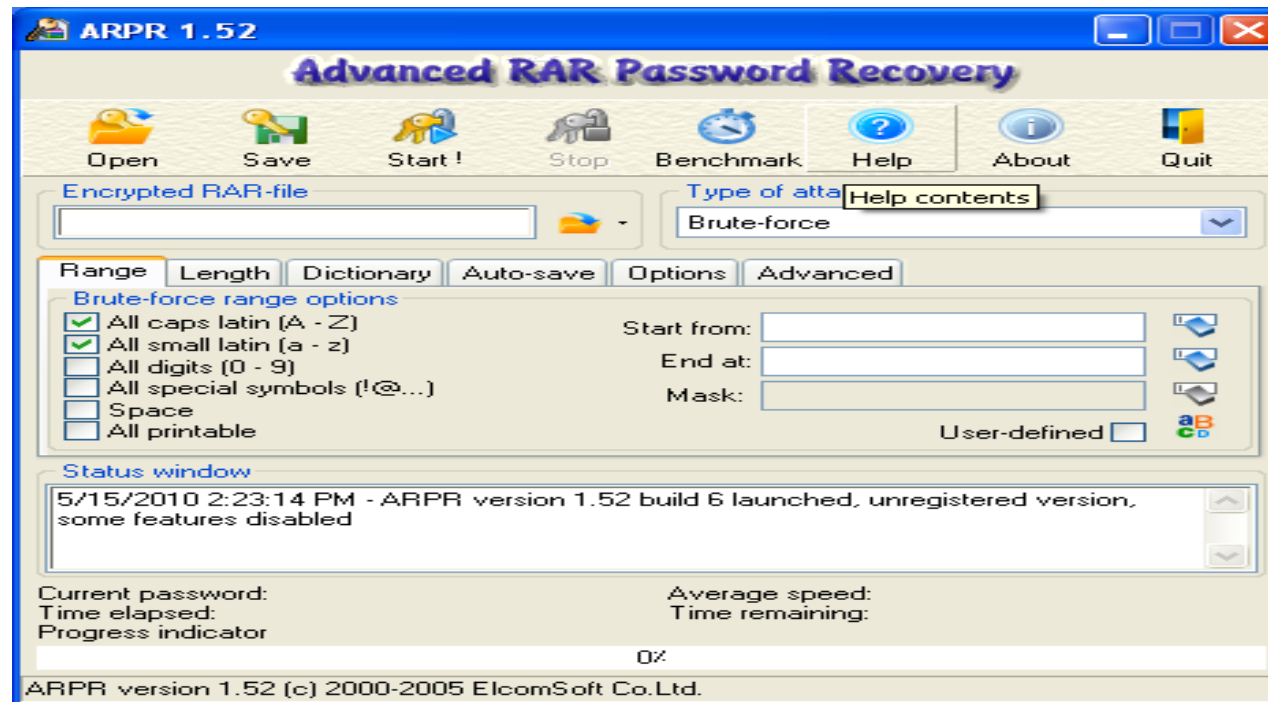
Passwords Likely for a User (count)

- Several network sites post dictionaries of phrases, science fiction characters, places, mythological names, Chinese words, and other specialized lists.
- All these lists are posted to help site administrators identify users who have chosen weak passwords.
- but the same dictionaries can also be used by attackers of sites



Passwords Likely for a User (count)

- Now Internet sites offer so-called password recovery software as freeware or shareware.



Summary

In this lecture we talked about :

- User authentication and its definition and we know that it is the process of verifying an identity claimed by or for a system entity.
- The most common authentication mechanism for user to operating system is a password.
- We discussed the access control
- We discussed the Probable Passwords and the Passwords Likely for a User

