

APNIC

Agenda



- Define access control and list the four access control models
- Describe logical access control methods
- Password Control

Acknowledgement



- Jamie Gillespie (APNIC)
- Security+ Guide to Network Security Fundamentals, Third Edition

Access Control



Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Security reads badge to determine it is real	User provides password
Authorisation	Permission granted for admittance	Security opens door to allow person in	User authorised to log in
Access	Right given to access specific resources	Delivery person can only retrieve parcel	User allowed to access specific data

Access Control

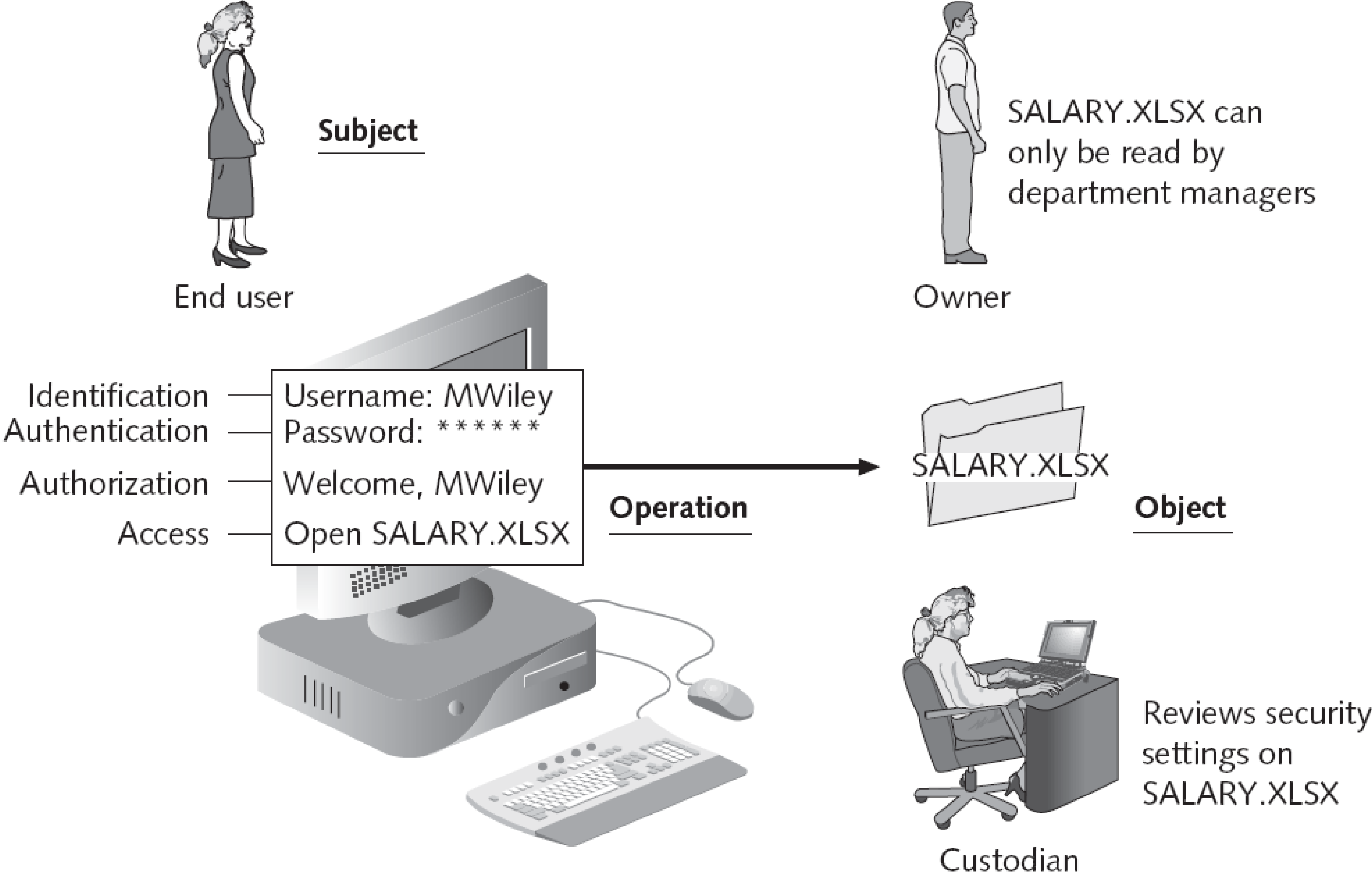
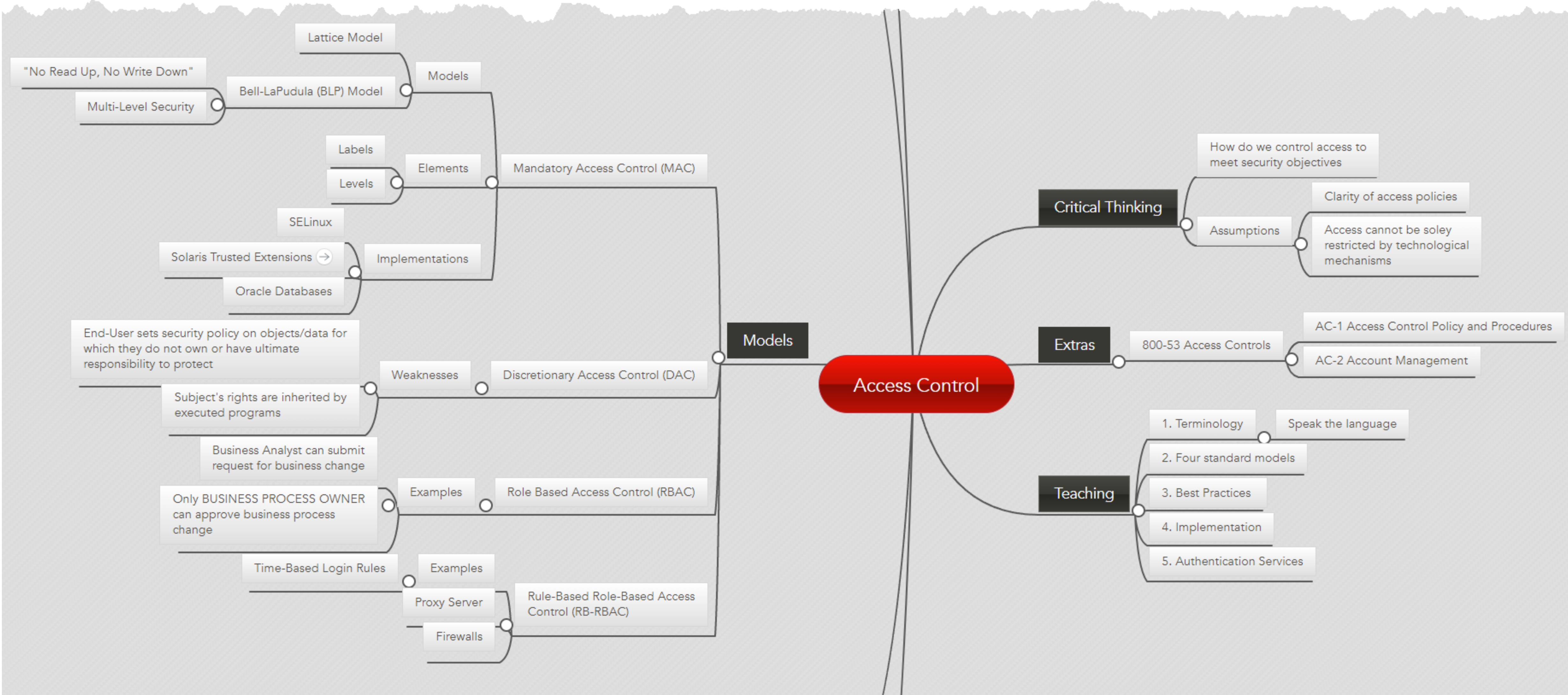


Figure 7-1 Access control process and terminology

https://cap430.files.wordpress.com/2011/04/ch07_accesscontrolfundamentals1.pdf

Access Control

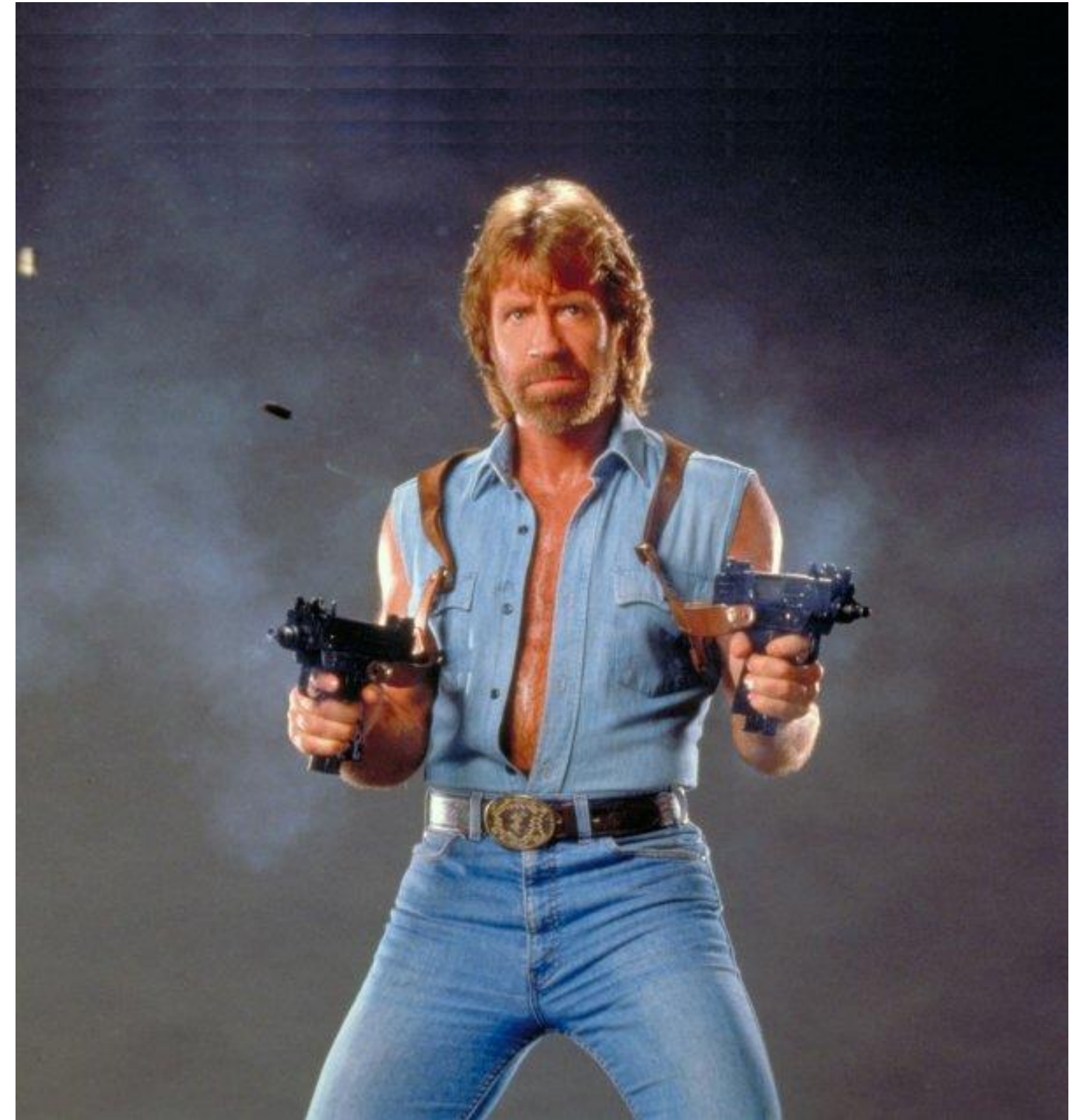


<https://www.mindmeister.com/286358115/access-control?fullscreen=1>

Access Control – Night Club



- Authentication
 - ID Check
- Access Control
 - Over 18 -> allowed in
 - Over 21 -> allowed to drink
 - On VIP List -> access all areas
- Enforcement Mechanism
 - Walls, Doors, Locks, Bouncers



<https://makeameme.org/media/templates/chuck-norris.jpg>

Access Control – Night Club



- Tickets
 - Name or anonymous
 - Date



- What if you want to leave and come back
 - Hand stamp or bracelet



<https://www.speedystamps.co.uk/blog/wp-content/uploads/2012/02/hand-stamps.jpg>

Access Control Models



- Mandatory Access Control
- Discretionary Access Control
- Role-Based Access Control
- Rule-Based Access Control

Access Control



Name	Restrictions	Description
Mandatory Access Control (MAC)	End User cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organisation and then users are assigned to roles	Considered a more “real world” approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Logical Access Control Methods



- The methods to implement access control are divided into two broad categories
 - Physical access control
 - Logical access control
- Logical access control includes access control lists (ACLs), group policies, account restrictions, and passwords

Access Control Lists (ACL)



- Access control list (ACL)
 - A set of permissions that is attached to an object
 - Specifies which subjects are allowed to access the object
 - And what operations they can perform on it
- These lists are most often viewed in relation to files maintained by the operating system
- Access control entry (ACE)
 - Each entry in the ACL table in the Microsoft Windows, Linux, and Mac OS X operating systems

Account Restrictions



- Time of day restrictions
 - Limit when a user can log on to a system
 - These restrictions can be set through a Group Policy
 - Can also be set on individual systems
- Account expiration
 - The process of setting a user's account to expire
 - Orphaned accounts are user accounts that remain active after an employee has left an organization
 - Can be controlled using account expiration
- Password
 - The most common logical access control
 - Sometimes referred to as a logical token – A secret combination of letters and numbers that only the user knows

Module 2: Passwords

Password Control



- What makes a bad password
 - 8 characters long (or less, such as a PIN of 4 digits long)
 - A wild mix of upper case, lower case, number, and special characters
 - 30 day mandatory password rotation (even 90 days is rough)
 - Make sure to setup “secret questions” in case you forget your password

... wait, weren't these the “good” recommendations?!?

Test Your Password		Minimum Requirements			
Password:	<input type="text" value="Pa55word"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols			
Hide:	<input type="checkbox"/>				
Score:	<div style="width: 62%; background-color: yellow;">62%</div>				
Complexity:	Strong				
Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	$+(n*4)$	8	+ 32
✓	Uppercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)*2$	1	+ 14
⊗	Lowercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)*2$	5	+ 6
⊗	Numbers	Cond	$+(n*4)$	2	+ 8
✗	Symbols	Flat	$+(n*6)$	0	0
⊗	Middle Numbers or Symbols	Flat	$+(n*2)$	2	+ 4
✓	Requirements	Flat	$+(n*2)$	4	+ 8
Deductions		Type	Rate	Count	Bonus
✓	Letters Only	Flat	$-n$	0	0
✓	Numbers Only	Flat	$-n$	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 2
✓	Consecutive Uppercase Letters	Flat	$-(n*2)$	0	0
!	Consecutive Lowercase Letters	Flat	$-(n*2)$	3	- 6
!	Consecutive Numbers	Flat	$-(n*2)$	1	- 2

<http://www.passwordmeter.com>

Passwords



Lowercase = 26

+ Uppercase = 52

+ Numbers = 62

+ Special = 94

EFF long list = 7776

for using 6 dice

EFF short list = 1296

for using 4 dice

Top-Left Panel: Shows a password 'Tr0ub4dor &3' with annotations: 'UNCOMMON (NON-GIBBERISH) BASE WORD' (16 boxes), 'ORDER UNKNOWN' (1 box), 'CAPS?' (1 box), 'COMMON SUBSTITUTIONS' (3 boxes), 'NUMERAL' (2 boxes), and 'PUNCTUATION' (4 boxes). A note says: '(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)'

Top-Right Panel: '~28 BITS OF ENTROPY' (16 boxes), '2²⁸ = 3 DAYS AT 1000 GUESSES/SEC' (16 boxes), and '(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)'. 'DIFFICULTY TO GUESS: EASY'. A comic character asks: 'WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO? AND THERE WAS SOME SYMBOL...'

Bottom-Left Panel: Shows the password 'correct horse battery staple' with annotations: 'FOUR RANDOM COMMON WORDS' (4 boxes). '~44 BITS OF ENTROPY' (16 boxes), '2⁴⁴ = 550 YEARS AT 1000 GUESSES/SEC' (16 boxes), and 'DIFFICULTY TO GUESS: HARD'.

Bottom-Right Panel: A comic character says 'THAT'S A BATTERY STAPLE.' and 'CORRECT!' with a battery icon. 'DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT'.

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passwords



The top table shows the number of possible passwords, using $(\text{characters})^{\text{length}}$
i.e. $(26)^3 = 17,576$

Length	10 Numbers	26 Character	52 Character	94 Character	1296 Words	7776 Words
1	10	26	52	94	1296	7776
2	100	676	2704	8836	1679616	60466176
3	1000	17576	140608	830584	2.177E+09	4.702E+11
4	10000	456976	7311616	78074896	2.821E+12	3.656E+15
5	100000	11881376	380204032	7.339E+09	3.656E+15	2.843E+19
6	1000000	308915776	1.977E+10	6.899E+11	4.738E+18	2.211E+23
7	10000000	8.032E+09	1.028E+12	6.485E+13	6.141E+21	1.719E+27
8	100000000	2.088E+11	5.346E+13	6.096E+15	7.959E+24	1.337E+31
9	1E+09	5.43E+12	2.78E+15	5.73E+17	1.031E+28	1.039E+35
10	1E+10	1.412E+14	1.446E+17	5.386E+19	1.337E+31	8.083E+38

The bottom table shows the password complexity as entropy, using $\log_2(\text{num of passwords})$

Length	10 Numbers	26 Characters	52 Characters	94 Characters	1296 Words	7776 Words
1	3	5	6	7	10	13
2	7	9	11	13	21	26
3	10	14	17	20	31	39
4	13	19	23	26	41	52
5	17	24	29	33	52	65
6	20	28	34	39	62	78
7	23	33	40	46	72	90
8	27	38	46	52	83	103
9	30	42	51	59	93	116
10	33	47	57	66	103	129

<https://generatepasswords.org/how-to-calculate-entropy/>

What makes a good password



- Longer is stronger (usually*). 15 character passphrases *should* be normal, and 30+ for more sensitive sites
 - * “usually” means that if you force users to use 16 character passwords and they don’t use a password manager, then you’ll get passwords like: fourfourfourfour or passwordpassword
 - “should” is my perfect world full of rainbows and unicorns, and where everyone is secure
- Choosing 4 (or more) random words gives you a strong password that humans can remember (see XKCD comic on next slide)
- To increase the complexity, break up a word by putting a number in the middle of it and/or using something other than a space between words
 - some password crackers use dictionary words and assume spaces between words as a way to break passwords faster

What makes a good password



- Longer is stronger... (1/3)
 - Problem: humans are bad at selecting random words (or random anything)
 - Solution: use the EFF's large list
 - References and background reading:
 - <https://www.eff.org/dice>
 - <https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases>
 - If you don't have dice handy, use <https://www.random.org/dice/>
 - Exercise: Open up the long list and random dice URLs above to create some passphrases

What makes a good password



- Passwords should be globally unique across all sites, both internal and external
 - Problem: humans are bad at remembering 40+ unique 12 character long passwords
 - Solution: use a password manager
- Better solution: use a password manager with completely random passwords using maximum character sets
 - Although you still need a memorable master password for your password manager, so keep those dice handy
 - We discuss password managers in a few slides

What Makes a Good Password

- Passwords may need to be rotated, either for compliance (☹️) or after a web site has been compromised ^(1/2)
 - Password resets can exhaust your users, especially if they are not using password managers
 - Ref: <https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/> and the longer article at <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>

What Makes a Good Password

- Passwords may need to be rotated (2/2)
 - Password manager helps here too, as you don't need to remember the new rotated password
 - New passwords should be randomly generated so you don't have users introducing weakness by creating password variations
 - Password1, Password2, Password3 PasswordJan, PasswordFeb, PasswordMar
 - PasswordGoogle, PasswordYahoo, PasswordEbay, PasswordLinkedin
- One university study found that 17% of new passwords could be guessed easily by knowing what the previous password was. 50% could be guessed within a few seconds of a computer trying
 - Ref: <https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf>

Password Control

- Password managers
 - Many to choose from, each with different features and options.
 - Some use cloud storage for easy sync between devices, but also makes it possible to attack remotely
 - Some use 2FA and source-country restrictions for logins to limit the above-mentioned issue, but this can increase the complexity for average users
 - Some are non-cloud based to mitigate remote attacks, but then makes it difficult to sync between devices, and would require something like Dropbox or Google Drive
 - Determine your threat profile to help you choose which password manager is best for you
 - In the end, password managers don't have to be perfect, they just need to be better than not using one!
 - The best password to use is one that you can't remember
 - People gave away their passwords for a pen (social engineering)

Password Control

- Server Side Passwords
 - If you are running a server that requires users to create accounts and passwords, you are in a very unique situation to either make the password problem worse, or better.
 - Most of the following recommendations are from the updated NIST document 800-63B on Digital Identity Guidelines
 - <https://pages.nist.gov/800-63-3/sp800-63b.html>

Server Side Passwords

DON'T force arbitrarily short passwords

- Why do some sites restrict you to a maximum of 16 characters?
- When you hash a password, the output will always be the same length irrespective of how long the input is, so the storage of a hashed password will be a known length for the database.
- You can set the minimum password length to something reasonable like 8 or 10 characters, but do not restrict the maximum length to less than 64 characters. Some sites allow up to 128 or 200 characters.

Server Side Passwords



DON'T exclude which characters can be used.

- This is done by lazy programmers that don't sanitize the user's input before it is processed or stored (usually in a database as plaintext)
- This breaks password managers creating random passwords, frustrating your users who are trying to be more secure.

• Similarly, **DON'T** force which characters **MUST** be used.


- This just makes things hard for the user without applying any real test to the strength of the password.

Server Side Passwords

DON'T force periodic password resets or expiry

- This just frustrates everyone
- As mentioned earlier, some compliance standards and auditors will tell you this is required. Use the research info from earlier slides to explain the current state of password control. Sometimes auditors will allow for exceptions or compensating controls which may allow you to get around forced rotation (or at least short reset periods).
And we can always hope for standards to get updated with new info!

Server Side Passwords

-  **DON'T** use “forgotten password questions/answers”, “secret questions”, or “knowledge based authentication”
 - This is usually the fastest way for an attacker to compromise an account.
 - Most information being asked can be found on Facebook accounts
 - Where did you grow up?
 - What is your oldest sibling’s name?
 - Other questions are just plain weak
 - What is your favourite colour?

Server Side Passwords

DO ensure you are storing passwords safely

- Previously this meant hashing a password, but as we'll discuss in the cryptography module, normal hashing is no longer sufficient
- Add a salt to your hashes
- Change the salt for every password, every single time
- Use a hashing algorithm that lets you define the work factor, and increase it over time
- Ref: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

Server Side Passwords



DO check new passwords against a list of known-compromised passwords and force the user to try again if any match (1/2)

- <https://haveibeenpwned.com/Passwords>
 - There's an API available, or you can download the 517 million compromised passwords (as SHA1 or NTLM hashes) in a 10.3GB compressed file if you want to check passwords locally.
 - Background reading from the guy making the above site available, Troy Hunt
<https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/>
- Exercise: Go to the above URL and test a weak password and a strong password, but don't use any of your current/valid passwords as this is still an external site!

Server Side Passwords



DO check new passwords against a list of known-compromised passwords (2/2)

- If you can't implement checks against the HIBP list, or if you want to do additional checks for password strength, consider something like “zxcvbn”
 - <https://github.com/dropbox/zxcvbn>
zxcvbn is open source software created by Dropbox, and their USENIX paper is linked at the top of the GitHub link
- Exercise 2: Go to <http://192.168.30.1/Exercises/zxcvbn/> and test some different fake passwords against the zxcvbn checker tool.
Public copy of the zxcvbn tool is at <https://lowe.github.io/tryzxcvbn/>


Server Side Passwords



DO provide Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)

- And DO encourage or require it to be enabled for users.
- Microsoft forces users to have one out of band factor verified (e.g. mobile phone, secondary email) and regularly prompts the user to confirm they are still valid.
 - Password reset success went from 67% to 93%
 - Recovery of compromised accounts went from 57% to 81%

Server Side Passwords

-  **DO** notify your users if someone tried logging into their account with the correct password but an incorrect 2FA/MFA code
 - This is a clear sign that the user's password is compromised and they should change it

Server Side Passwords

- Exercise: Can you spot the problems with the following password restrictions?
 - Most of these are from 2012-2016, and only some have been fixed

Change My Password



Change your password

The password you create here can be used to access Online, Mobile and Telephone Banking.

All passwords must be six characters in length. Special characters (eg. *, %, \$, etc) will not be accepted. Choose a password that's easy for you to remember, but difficult for others to guess. Avoid using birthdates, your name or initials, common phrases such as 'abc123' or passwords you have created for other systems. Do not keep a reminder of your password in an easily accessible place.

All fields are required

Enter your current password: *

Enter your new password:  

Re-enter your new password:

Your password must be exactly 6 characters in length. Enter only letters and/or numbers.

Change Password

Enter Current Password

Choose a New Password

Password strength:



Confirm your Password

[Cancel](#)

[Change](#)

Your Password must:

- Be 6 - 50 characters with at least 1 letter AND 1 number

Your Password must not:

- Contain any spaces or more than 2 consecutive identical characters
- Be the same as your User ID
- Have any spaces before, in the middle of, or following any characters
- NOTE: Password is not case sensitive

[x Close](#)



MY ACCOUNT

CARDS

TRAVEL

INSURANCE

REWARDS

BUSINESS

United Kingdom (Change Country) Contact Us

LOGOUT

Need help?



Account Home

Your Statement

Payments

Profile & Preferences

Information & Help

Card Management

Profile & Preferences

Summary

Contact Details

Statement Delivery

Card Alerts

Marketing Preferences

Login Password

Change Login Password

The password applies to your entire Online Services Account and is not Card specific.

Enter current password *

Enter new password *

Re-enter new password *

* Required fields

[Clear details](#)

Your password:

- Must be different from your User ID.
- Must contain 8 to 20 characters including one letter and number.
- May include the following characters: % & _ ? # = -
- Your new password cannot have any spaces and will not be case sensitive.

CHANGE YOUR PASSWORD



Step: **1** — 2

- Updates to your online banking password will take effect immediately.
- Changing your Online Banking password will not affect your telephone banking password.

CIBC card: 4506 4464 6653 3011

Current password:

New password:

Password strength:



Show password

! Please enter a password that is 6 to 12 characters long and is made up of any combination of numbers, English letters or both.
{Result #0015}

Re-enter password:

Logout



Enter your Pincode



1

2

3

ABC

DEF

4

5

6

GHI

JKL

MNO

7

8

9

PQRS

TUV

WXYZ

0



Password Tips & Tricks

- In addition to using strong passwords and using 2FA, here's a couple of things you can do to add a little extra assurance to your passwords...

Password Tips & Tricks

- On the haveibeenpwned.com site you can subscribe your individual email address or for an entire domain to be alerted for any new data breaches exposing your passwords
 - To verify ownership of a domain, you will need to produce one of:
 - Email verification to `security@`, `hostmaster@`, `postmaster@`, or `webmaster@`
 - Meta tag on your web server root index page
 - A special file uploaded to the root of your web server
 - DNS TXT record
 - Ref: <https://haveibeenpwned.com/DomainSearch>
 - To verify ownership of an email address, you just need to respond to a verification email
 - Ref: <https://haveibeenpwned.com/NotifyMe>

Password Tips & Tricks

- When creating passwords to be used inside a company, consider prepending the randomly generated password with /!
 - The / (slash) as the first character will prevent the password from accidentally being pasted into IRC or Slack channels or direct messages (IRC/Slack will think it is a command)
 - The ! (exclamation mark) will prevent the password from being saved as a command in the history/bash_history file if you paste your password into a Linux shell
 - This can make it tricky (using quotes, escaping) if you need to embed your password into a command line such as running mysql with a password, but using passwords on command lines is not good security practice anyways, so don't do that!
 - This also assumes you have history expansion turned on, which it is by default. If history expansion is turned off, your password will be saved in history

Password Tips & Tricks

- Exercise: Log into Kali, open a terminal/console window and type in the following two “passwords” (press enter after each)

!ABC123 (no spaces)

XYZ789

- Now run the following command to view command history

history

- You can also press the up and down arrow keys to see previous commands

Module 3: Operational Security

- Least privilege
 - Only give the amount of access required to get the job done
 - Not just for users but also for services and applications
 - This applies to all aspects of life and security
 - Office buildings
 - Mobile phone apps
 - Servers, routers
 - Firewall policies
 - Service account used for web application to access SQL DB
 - User access to file systems (think ransomware)
 - Easiest to implement least privilege by using Role Based Access Control (RBAC)
 - All network engineers need the same access
 - Create an access group for those privileges
 - Assign access group to all network engineers
 - Makes handling exceptions easier

Operational Security



- Following least privilege also means that administrators should have 2 accounts
 - One for daily activities like web browsing and email
 - One for administrative tasks like creating new user accounts or assigning new permissions
- Create an Employee exit procedure
 - If someone no longer works at the organisation, they don't have a need for access privileges (least privilege = nil)
 - This is exploited in the movie *Minority Report*, where the police officer still has access to the HQ building even after he is convicted and sentenced for murder

- Regular review of assigned access privileges (1/2)
 - Examples
 - Employee starts in one department or doing one role
 - Occasional moves to a different role, gaining more access
 - “Temporary” access granted for special projects, but never revoked
 - If using RBAC, this can be as simple as contacting the manager for a group of employees and having them confirm that their direct reports still require current granted access

- Regular review of assigned access privileges (2/2)
 - And/or have owners for each RBAC group, then regularly access the access group manager to confirm that the members of that access group are still allowed to be in the group
 - Example: a “Network Engineers” access group could have the manager or network architect as the owner of the group
 - Works best when you have accurate role descriptions for employees
 - Most compliance requires dictate reviews every 6-12 months

- Be careful with default configurations
 - Default configurations are usually just for examples or learning, not for production
 - Default passwords should always be changed
 - Usually best to wipe default configs completely and start from scratch
 - IoT falls into this recommendation

Operational Security



- Don't save unencrypted passwords anywhere (1/2)
 - A text file on your desktop or home directory is not a good place to store passwords
 - Neither is:
 - vnc.ini
 - sysprep.inf, sysprep.xml, or unattend.txt
 - Anywhere found by using: `grep` or `find /l "password" *.txt` (or `*.ini`, `*.xml`)
 - Internal (or external!) doc sites, wikis, CMS, etc...
 - Don't forget about revision history after you try to remove passwords from documentation.
 - Registry entries
 - Saved sessions for FTP or SSH applications
 - GitHub
 - `.history` or `.bash_history`

- Don't save unencrypted passwords anywhere (2/2)
 - Attackers (and penetration testers) know where to look for passwords, scripts can do this automatically, quickly, and auto-decrypt files
 - Ref: Encyclopaedia Of Windows Privilege Escalation at <https://www.insomniasec.com/releases>
 - If a password is ever exposed in plaintext, it should be changed/rotated. Even if it doesn't appear to have been viewed or copied by anyone.
 - Typing work password into non-work website
 - Typing password into bash shell
 - Saving passwords in GitHub or CMS systems

- Shred everything
 - Use a cross-cut shredder, strips can be reassembled
 - Dumpster diving is an old concept but still used today
 - People are bad at assessing the risks of disposing information by different means
 - Reduce the average person's decision making
 - All paper is shredded or put in a secure bin for shredding/destruction
 - All hard drives are securely wiped between use
 - All hard drives are extra wiped or physically destroyed before leaving the organisation

- **Encrypt everything**
 - If there is ever an option, choose to go with encryption
 - Laptops being taken out of the office/country
 - Encrypted Wi-Fi access points
 - Mail server to mail server
 - Administrative access to servers and consoles
 - Password storage
 - Make sure you have policies and procedures to avoid problems
 - Encrypted hard drives means if the key is lost, it's almost equivalent to securely wiping the drive

Operational Security

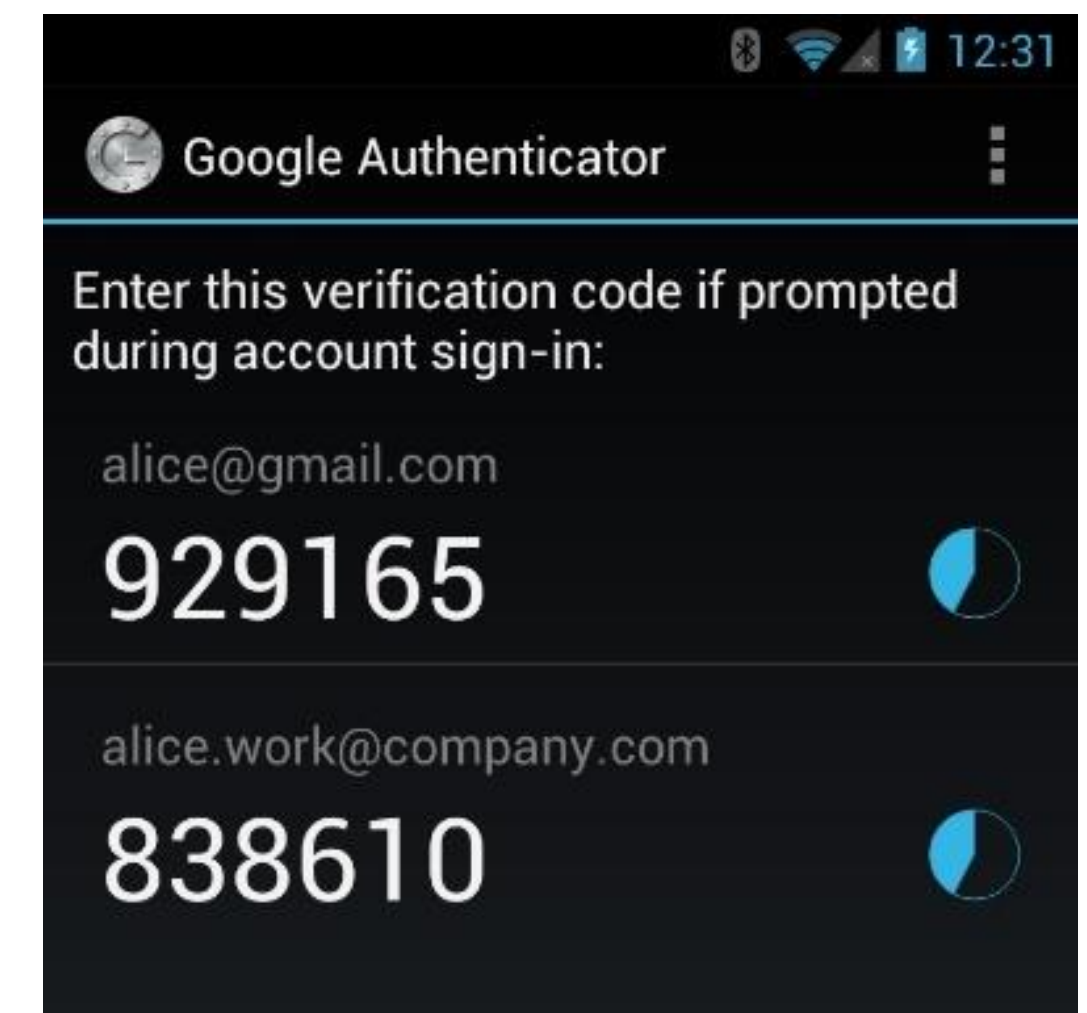
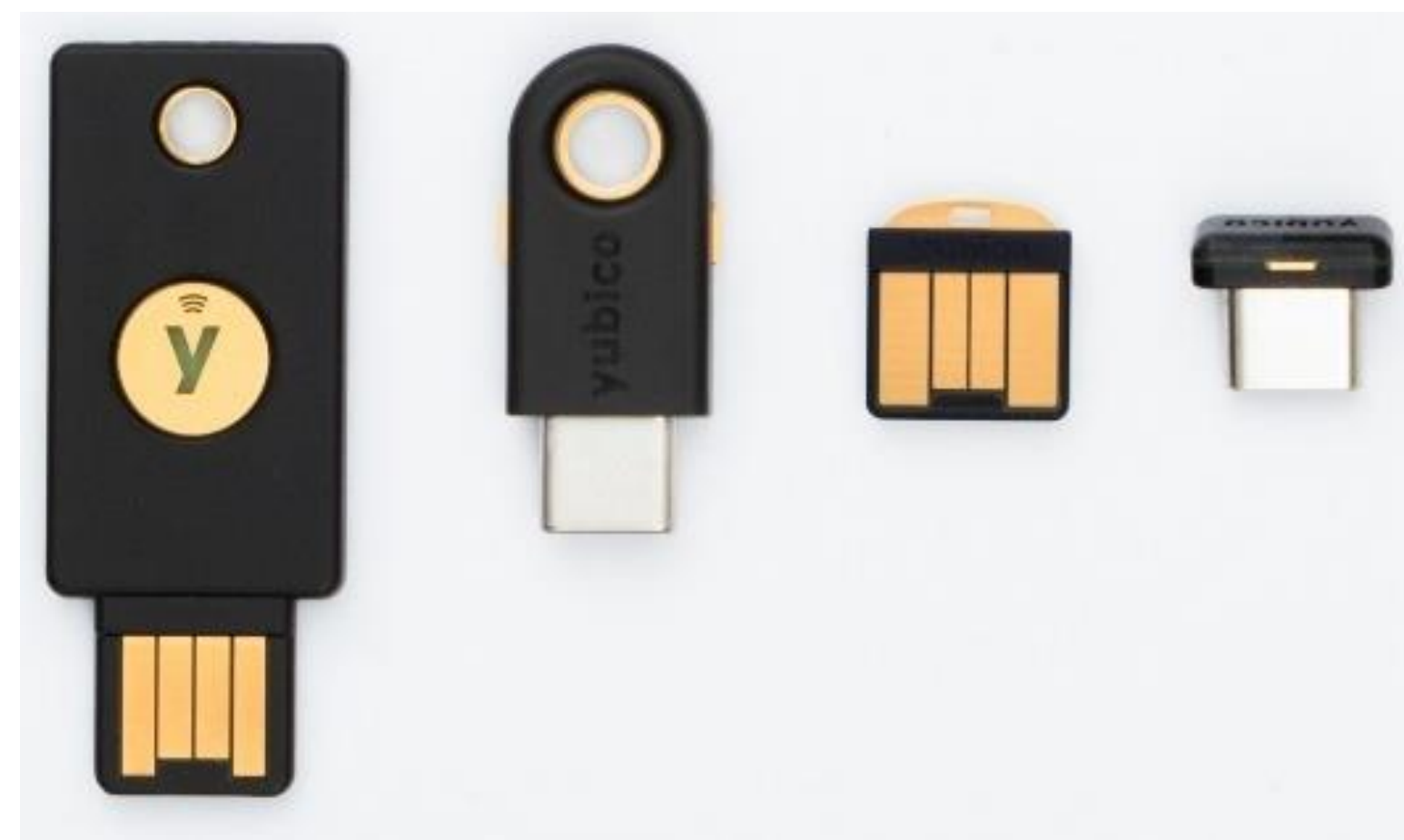


- 2FA everything
 - If there is ever an option, enable 2FA
 - Without 2FA, someone only needs to guess or shoulder-surf your password, usually from anywhere in the world

2FA = 2 Factor Authentication

MFA = Multifactor Authentication

2SV = 2 Step Verification



<https://www.okta.com/blog/2021/07/what-is-two-factor-authentication-2fa/>

Operational Security



- Multifactor Authentication (MFA)

MFA factor type comparison

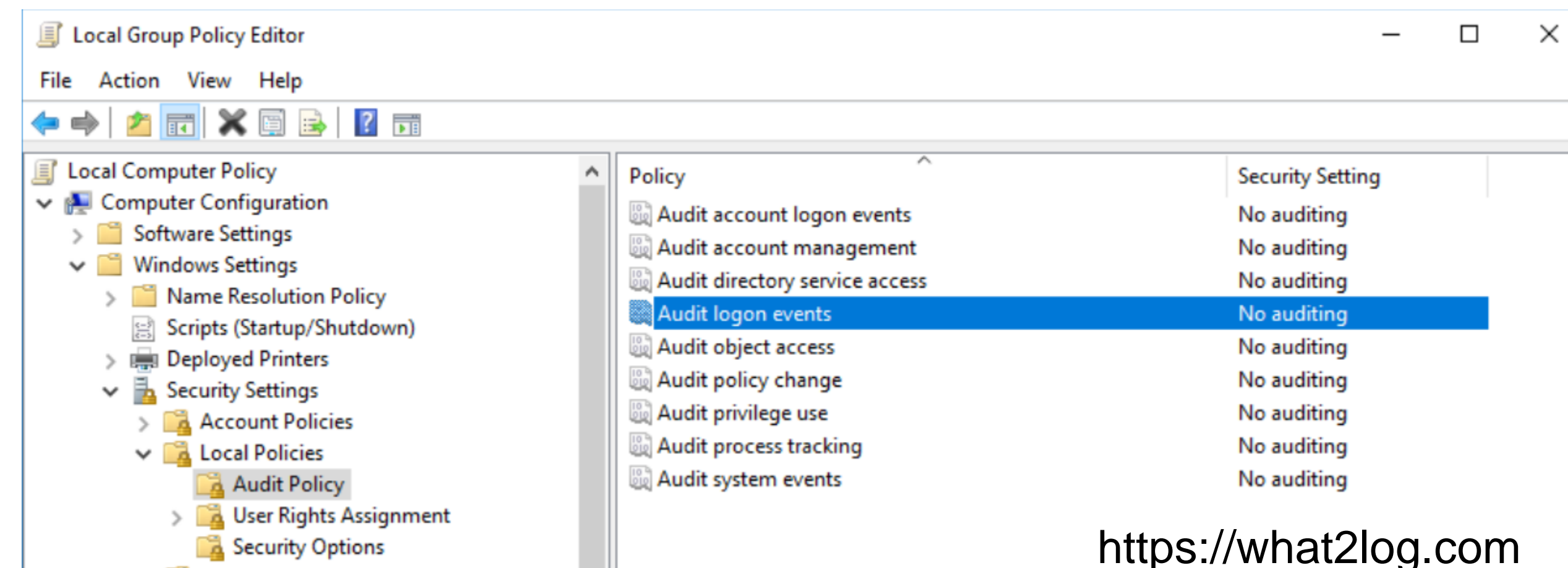
Factor Type	Security	Deployability	Usability	Phishing Resistance	Real-Time MITM Resistance
Passwords	Weak	Strong	Strong	Weak	Weak
Security Questions	Weak	Strong	Moderate	Weak	Weak
SMS / Voice / Email	Moderate	Strong	Strong	Moderate	Weak
Push Verification	Strong	Strong	Strong	Strong	Moderate
YubiKey OTP	Strong	Strong	Strong	Moderate	Weak
WebAuthn	Strong	Moderate	Strong	Strong	Strong

<https://help.okta.com/en/prod/Content/Topics/Security/mfa/about-mfa.htm>

Operational Security



- Log everything
 - You don't know if you need logs until after an event, then it's too late
 - You don't know if something happened unless you log it
 - Even then, you don't know if something happened unless you review your logs
 - Not all logs are created equal, and not all logs need to be retained for the same time
 - Centralising your logs takes it to the next level



<https://what2log.com>

- Automate everything
 - If you must do a task more than a couple of times, you should at least partially automate it
 - This may involve an additional up-front cost to the organisation, but is usually easy to justify

Operational Security



- Document everything
 - Security policies, procedures, projects/systems
 - For your users, for yourself, and for your manager who has to deal with it when you win the lottery and retire early

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\warren> Start-Transcript
Transcript started, output file is C:\Users\warren\OneDrive - APNIC\Documents\PowerShell_transcript.WARREN-802593.M4KrUd
Dm.20211219125732.txt
PS C:\Users\warren> Get-Date

Sunday, 19 December 2021 12:57:44 PM

PS C:\Users\warren> Stop-Transcript
Transcript stopped, output file is C:\Users\warren\OneDrive - APNIC\Documents\PowerShell_transcript.WARREN-802593.M4KrUd
Dm.20211219125732.txt
PS C:\Users\warren> |
```

```
1 *****
2 Windows PowerShell transcript start
3 Start time: 20211219125732
4 Username: ORG\warren
5 RunAs User: ORG\warren
6 Configuration Name:
7 Machine: WARREN-802593 (Microsoft Windows NT 10.0.19043.0)
8 Host Application: powershell.exe
9 Process ID: 23988
10 PSVersion: 5.1.19041.1320
11 PSEdition: Desktop
12 PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1320
13 BuildVersion: 10.0.19041.1320
14 CLRVersion: 4.0.30319.42000
15 WSMANStackVersion: 3.0
16 PSRemotingProtocolVersion: 2.3
17 SerializationVersion: 1.1.0.1
18 *****
19 Transcript started, output file is C:\Users\warren\OneDrive - APNIC\Documents\PowerShell_transcript.WARREN-802593.M4KrUd
20 PS C:\Users\warren> Get-Date
21
22 Sunday, 19 December 2021 12:57:44 PM
23
24
25 PS C:\Users\warren> Stop-Transcript
26 *****
27 Windows PowerShell transcript end
28 End time: 20211219125802
29 *****
30
```

<https://adamtheautomator.com/powershell-logging-2/>

- Backup everything
 - If it has any value at all, back it up
 - We don't value many things until there are gone
 - That's a bit deep, so it's ok if you want to take a break to call your family :)
 - Schrodinger's Backup – you don't know if a backup is good or not until you test it
 - Just because a backup was successful, doesn't mean the restore will be. A lot of things can happen to the backup media after a backup.