Introduzione a Windows

Lezione 3

Best Practice per la Sicurezza

Ruggero Donida Labati

Laboratorio di Sistemi Operativi

Università degli Studi di Milano
Dipartimento di Informatica
A.A. 2024/2025

Panoramica della lezione

- A titolo di approfondimento, verranno descritte alcune best practices per la messa in sicurezza di personal computers con sistema operativo Windows 10

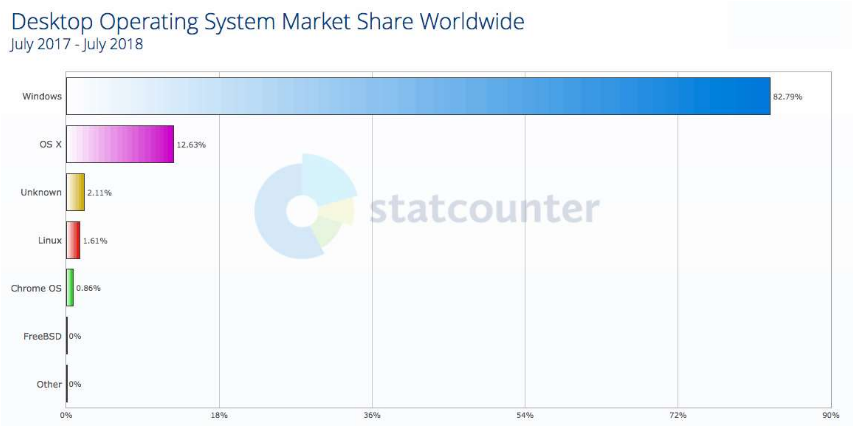
Sommario

1. Hardening Windows
2. Some best practices
3. Credits

1. Hardening Windows

Why should we study protection mechanisms?

- Windows is the most used OS for personal computers



Desktop Operating System Market Share Worldwide
July 2017 - July 2018

Hardening Windows

- Hardening your Windows 10 computer means that you’re configuring the security settings
  - This reduces opportunities for a virus, hacker, ransomware, or another kind of cyberattack

- You can think about security for your computer, much like you’d think about security for your house
  - Hardening your PC is like you’re closing the doors and checking the locks
  - You want to make it harder for hackers to break in

2. Some best practices

Disable Windows 10 automatic login

- If anyone can open your computer, it can create a serious security risk
  - This is especially important if you travel with a laptop

- How to
  1. Press **Win+R**, enter “**netplwiz**“, which will open the “**User Accounts**” window

     Netplwiz is a utility tool for managing user accounts
  2. Check the option for “**Users must enter a username and password to use this computer**” and click Apply
  3. Restart your computer

Set a password with your screensaver

- There's no reason someone in your office, home, or travel location should be able to access your system if you step away for a few minutes

- How to
  1. Open the **Control Panel**
  2. Click **Appearance and Personalization**
  3. Click **Change screen saver**
  4. In the Screen Saver Settings check the box "**On resume, display logon screen**"

Turn on your firewall (1/2)

- Network firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets
  - All messages entering or leaving the intranet would pass through the firewall, which examines each message and blocks any that don't meet the specified security criteria

- In recent versions of Windows operating systems, including Windows 10, your firewall is enabled by default

Turn on your firewall (2/2)

- How to

1. Open the Control Panel in Windows
2. Click on **System and Security**
3. Click on **Windows Firewall**
4. If your firewall is disabled, you'll see Windows Firewall marked "Off." To turn it on, in the left navigation pane, you can click on **Turn Windows Firewall on or off**
5. In the Customize Settings window, select **Turn on Windows Firewall** and click OK

Disable remote access (1/2)

- In Windows 10, you have the Windows Remote Desktop feature that allows you (or others) to connect to your computer remotely over a network connection
  - Remote access allows someone to control everything on your computer as if they are directly connected to it
- Unfortunately, hackers can exploit Windows Remote Desktop
  - In more than one cyberattack, criminals have gained to tried to gain control of remote systems, installed malware, or stolen databases full of personal information

Disable remote access (2/2)

- How to

1. Type “**remote settings**” into the Cortana search box
2. Select “**Allow remote access to your computer**”. This may seem counter-intuitive, but this opens the Control panel dialog for Remote System Properties
3. Check “**Don’t Allow Remote Connections**” to this Computer

Enable or install antivirus protection tools

- You can prevent viruses and malicious code using your built-in tools in Windows 10
- You can also install additional antivirus software if you need to

Enable auto-updates (1/2)

- You should install urgent security updates right away
  - Some securicy patches are critical fixes for protecting you from a new type of malware or cyberattack
  - Don’t be that person who ignores operating system updates for critical security patches

Enable auto-updates (2/2)

- How to
  1. Tap or click on the **Start button**, followed by **Settings**
  2. From Settings, tap or click on **Update & security**
  3. Choose **Windows Update** from the menu on the left, assuming it’s not already selected
  4. Tap or click on the **Advanced options** link on the right, which will open a window headlined **Choose how updates are installed**
  5. Select **Automatic (recommended)** from the drop-down, check “**Give me updates for other Microsoft products when I update Windows**”

Set up file backups (1/2)

- ○ Routine file backups are essential for protecting yourself from losing important data if you have a sudden hard-drive failure or your PC get a virus
  - You can use File History and other free tools in Windows 10 to create file backups.
  - You can create a recovery drive to restore your system from an image backup.
  - With a storage-sync-and-share service, you can put your backups in the cloud. These are easy to set up, especially some of the most popular ones like OneDrive, Dropbox, or Google Drive

Set up file backups (2/2)

- ○ Suggested solution
  - Incremental backup with daily frequency

- ○ Incremental backup software for Windows 10
  - Software provided by the vendors of external hard drives and NAS
  - Some free software solutions
    - Cobian Backup
    - Comodo BackUp
    - AOMEI Backupper Professional
    - Genie Timeline Free
    - Personal Backup

Turn on encryption (1/2)

- Goals
  - If your encrypted information were stolen, it would be unusable
  - Encrypting your entire drive also protects against unauthorized changes to your system, like firmware-level malware

- Soultion in Windows 10
  - BitLocker is Microsoft's proprietary disk encryption software, included with Windows 10
  - Bitlocker has you set a password, gives you a recovery key, and shows you an option to "Encrypt Entire Drive"

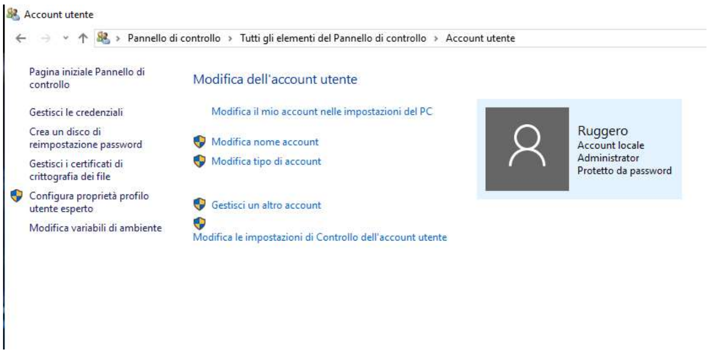
Turn on encryption (2/2)

- How to
  1. Locate the hard drive you want to encrypt under "**This PC**" in Windows Explorer
  2. Right-click the target drive and choose "**Turn on BitLocker**"
  3. Choose "**Enter a Password**"
  4. Enter a secure password
  5. Choose "**How to Enable Your Recovery Key**" which you'll use to access your drive if you lose your password. You can print it, save it as a file to your hard drive, save it as a file to a USB drive, or save the key to your Microsoft account
  6. Choose "**Encrypt Entire Drive".** This option is more secure and encrypts files you marked for deletion
  7. Unless you need your drive to be compatible with older Windows machines, choose "**New Encryption Mode**"
  8. Click "**Start Encrypting**" to begin the encryption process. Note that this will require a computer restart if you're encrypting your boot drive. The encryption will take some time, but it will run in the background, and you'll still be able to use your computer while it runs

Set up your user accounts (1/2)

- Types of accounts
  - Administrator Account
    - The first account on a Windows 10 PC is a member of the Administrators group and has the right to install software and modify the system configuration
  - Standard Account
    - You can use a Standard user account for your regular use, which limits access to the Administrator account, preventing a nontechnical user from inadvertently making changes to your system or helping block an unwanted software installation
  - Guest Account
    - By default, a Guest account has a blank password
    - Since the Guest account provides anonymous access to your computer, it is a security risk and a best practice to leave the Guest account disabled

Set up your user accounts (2/2)



Account utente

Pannello di controllo › Tutti gli elementi del Pannello di controllo › Account utente

Pagina iniziale Pannello di controllo

Gestisci le credenziali

Crea un disco di reimpostazione password

Gestisci i certificati di crittografia dei file

Configura proprietà profilo utente esperto

Modifica variabili di ambiente

Modifica dell'account utente

Modifica il mio account nelle impostazioni del PC

Modifica nome account

Modifica tipo di account

Gestisci un altro account

Modifica le impostazioni di Controllo dell'account utente

Ruggero
Account locale
Administrator
Protetto da password

Set up a password manager (1/2)

- If one password is stolen in a data breach, that password could then give nefarious actors access to multiple accounts with your personal, financial, or professional information
- As hackers are getting better and better at stealing or cracking passwords, technology companies are forcing us to make our passwords stronger and more complicated
  - That also means more people start re-using passwords

Set up a password manager (2/2)

- Windows 10 and your browser may have some features for saving passwords, but a best practice in the infosec world is to use a dedicated password manager
  - Password managers have you create a master password for your “vault” of sensitive accounts and login information
  - The best ones sync can automatically add new passwords, sync with your phone and computer, generate and autofill strong passwords, and let you share a specific password with coworkers or friends

5. Credits

Credits

○ D. Mac Leod, "Security Best Practices for Your Windows 10 Computer," *Building Your InfoSec Program*, November 2019, https://www.securicy.com/blog/security-best-practices-hardening-windows-10/

In sintesi

1. Hardening Windows
2. Some best practices
3. Credits