Lesson 5.1.2 End User System Security

DEVICE HARDENING

Device Hardening

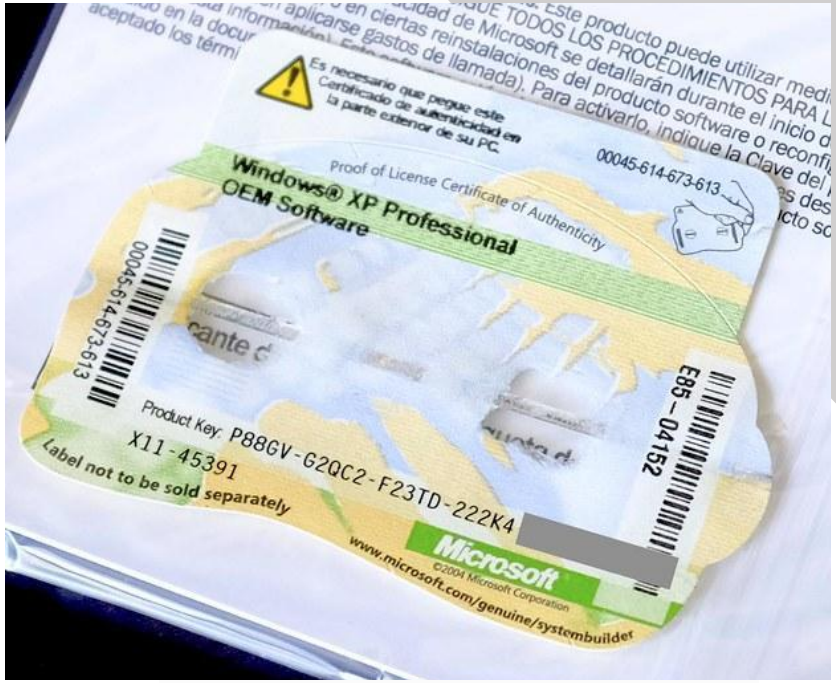
- Device hardening is a process to eliminate possible means of attack by patching vulnerabilities, turning off non-essential services, and configuring systems with security controls.
  - Hardware
  - Software
  - Mobile Devices

Hardware Hardening

- Set BIOS Password
  - Admin Password: Ensures BIOS settings, such as boot devices and order cannot be changed
  - User Password: The computer will not boot to the boot device without a password
- Disable Autoplay
  - Automatically starts certain programs on optical or removable devices
  - To turn it off
    1. Press the Windows key or click the Windows icon in the lower-left corner of your desktop.
    2. Type in autoplay and click on the AutoPlay Settings option.
    3. From this screen, toggle AutoPlay For All Media And Devices to Off. Also switch AutoPlay defaults for removable drives and memory cards to Take No Action.

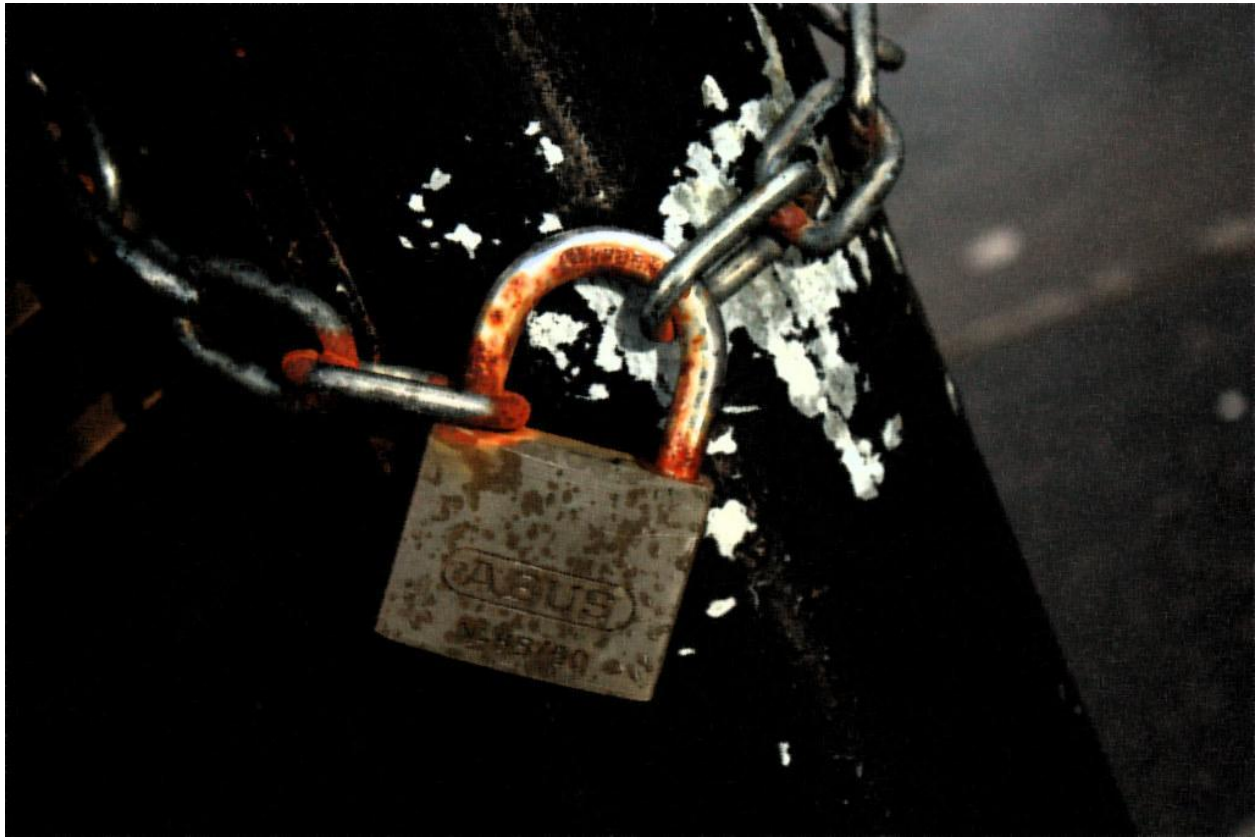
Software Hardening

- Licensing
  - Ensure you have a genuine licensed Operating System
  - Ensure your applications have genuine licensing
  - “Discount” applications and licenses are often at best fake, and at worst viruses and malware
  - Key or license generators are often Trojans in disguise
- Encryption
  - Ensures only authorized people can access data on your hard drive
  - For Windows 10, BitLocker is used
  - Removable devices can be encrypted via BitLocker To Go
    - Web browsers
      - Disable auto-loading ActiveX, Java, scripts and Plug-ins and use them sparingly
      - Delete Cookies on browser exit
      - Enable built in tracking protections and pop-up blockers

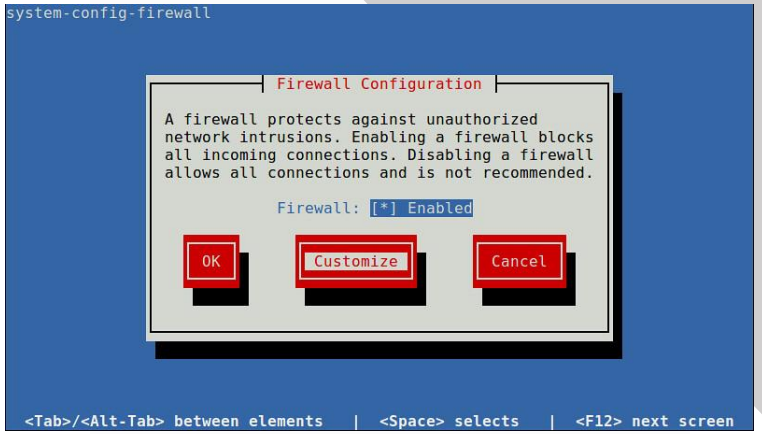


Software Hardening

- Lock the OS after *x* idle minutes and require a password to log in again
- Lock your computer whenever you leave your desk
- Uninstall inactive apps and features
- Check your privacy controls for every app and be aware about what you are giving permissions to
  - Location
  - Camera
  - Microphones



Software Hardening



- Windows Firewall and Network Protection
  - An important security application that's built into Windows.
    - Blocks unauthorized access to your computer
    - Permit authorized data communications to and from your computer
  - Private Network – At home or at work where you know and trust the people and devices on the network. Your device can be set up as discoverable.
  - Public Network – In a public place such as an airport or coffee shop where you don't know the people and devices on the network. Your device should not be set up as discoverable.
  - Allow Applications – You can allow certain trusted applications through the firewall
    - TeamViewer could be used to remotely access your PC.

Software Hardening

- Parental Controls
  - Web Sites
    - Can block inappropriate websites and force SafeSearch
    - Block or allow specific websites
  - Time Restrictions
    - Set start and end times as well as time limits (1 hour per day)
  - Reporting
    - Shows recent websites visited with time and date
  - Apps and Games
    - Block app, games, and media from the Windows Store by age

Mobile Devices

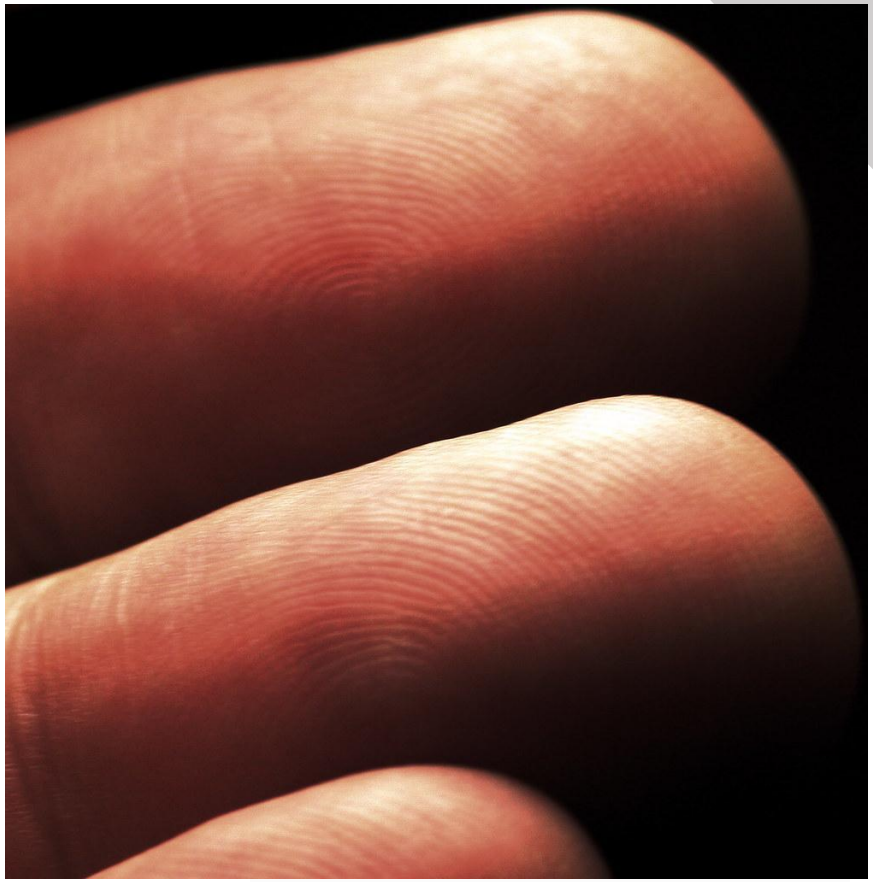
- Patches/Updates to OS
  - Devices ship with the most current version of the operating system available when the device was manufactured, but new updates often address security vulnerabilities in addition to bug fixes and adding new features.
- Patches/Updates to Apps
  - Application updates often address security vulnerabilities in addition to bug fixes and adding new features. It is recommended that applications, especially those used to interact with the internet and web-based services (e.g. Internet browsers) be updated frequently.

Mobile Devices

- Find my Phone
  - If a device is lost or stolen, having this service enabled may allow the owner to find and recover the device. Even if recovery of the device isn't possible, the ability to remotely erase it may protect any sensitive data that was stored on it.
- Passcode Lock
  - Setting a passcode prevents casual unauthorized access to a device. A passcode is also required in order to enable Data Protection and take full advantage of the encrypted storage of recent devices.

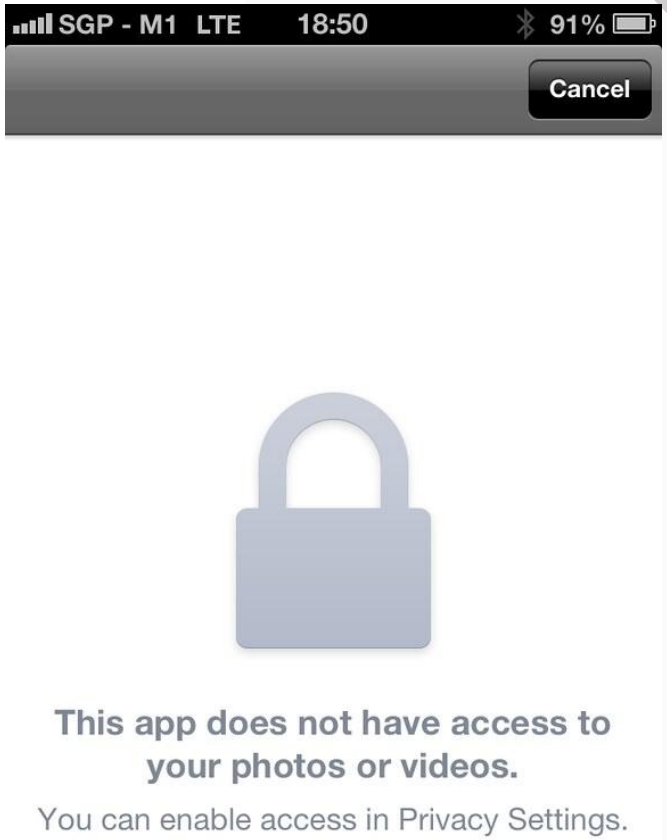
Mobile Devices

- Remote Wipe
  - The intent with this is to ensure that if the device is lost, the data can be erased remotely.
- Touch ID
  - Touch ID will allow you to authenticate to the phone without having to type in the password. Touch ID uses fingerprints.



Mobile Devices

- Backups
  - Backup data daily to ensure no data loss
- App Permissions
  - Pay attention to the location, microphone, and camera permissions you give apps
- Turn services off
  - Turn off services such as Bluetooth, AirDrop, and Personal Hotspots when not in use



Summary – Device Hardening

- Device Hardening
  - Hardware
  - Software
  - Mobile Devices