Locking Down a Publicly Accessible Windows PC

Things to do to protect the machine from the users and prevent more work for yourself
Why are the users the enemy?

- You have little or no control over who has access
- Some of the users will know what they’re doing and want more access
- Some of the users will be malicious
- Some just don’t know what they’re doing
Options for “securing”

- Built in operating system features
- First party add-ons
- Registry Hacks
- Third party applications
Windows Variations

- Windows 9x series
  - Windows 95
  - Windows 98
  - Windows 98SE
  - Windows ME

- Windows NT series
  - Windows NT 4
  - Windows 2000
  - Windows XP
Built in features

- Windows NT series
  - Use Computer Management under Administrative tools to create a public user account under the group “Guests”
  - Do not allow user to change password
  - Prevents user from deleting or renaming files
  - Prevents programs such as AOL from accessing modem drivers!
Built in features

- Windows 9x Series
  - No real security measures built in
  - Try first party add-ons
First Party Add-ons

- **Win9x**
  - Policy editor
  - TweakUI

- **WinNT**
  - TweakUI
Policy Editor

- Microsoft claims support only for Windows95
- Will work on Win98 and 98SE also
- Download from
Policy Editor

- Restrict user access to control panel features
- Restrict shell features
  - Remove Run, Settings, and Shutdown from Start Menu
- Restrict System functions
  - Disable access to command shell and registry editor
Policy Editor
TweakUI

- One version for Win9x, NT4, and Win2K
- One version for Windows XP
- One version for Windows XP SP1
- Download from
  - XP:
  - All others:
TweakUI

- Can be used to restrict access to control panel options
- Can be used to hide mapped drives in Windows Explorer
TweakUI for XP SP1

- Adds feature to restrict which users and groups can modify settings for things such as file and printer sharing
TweakUI for XP SP1
Hack the Registry

- Know What You Are Doing First!
- Improper registry settings can break Windows
Registry Editing

- Prevent user access to functionality which allows control over system
- Use registry to hide selected drives in Explorer
- Disable access to selected drives
- Disable access to command shell
- Disable registry editing
Registry Editing

- Prevent users from using My Computer or Explorer to access contents of drives. Also restricts Run, Map Network Drive, or the Dir command to view the directories.

- **User Key:**
  ```plaintext
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
  ```

- **System Key:**
  ```plaintext
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
  ```

- **Name:** NoViewOnDrive
- **Type:** REG_DWORD (DWORD Value)
- **Value:** 32-bit bitmask

- Bitmask is summation of hex values for each drive letter, A=1, B=2, C=4,D=8, etc.
Disable access to command shell in Windows

- **User Key:**
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]
- **System Key:**
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]
- **Name:** Disabled
- **Type:** REG_DWORD (DWORD Value)
- **Value:** (0 = disable, 1 = enable)
Registry Editing

- Prevent users from editing the registry
  - **Warning:** Be careful with this setting because once you enter this key into the registry you will not be able to use Regedit to undo the change.

- **User Key:**
  
  [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

  **Name:** DisableRegistryTools
  **Type:** REG_DWORD (DWORD Value)
  **Value:** (0 = allow regedit, 1 = disable regedit)
Segue Slide

- Locked out of the registry due to a setting you just applied?
- A third party utility such as WinGuides Tweak Manager can fix it.
- And now we transition to third party applications for securing Windows.
Third Party Applications

- Can be expensive
- Usually have discount prices for educational/government institutions and for site licenses
- Provide fancy GUIs for changing settings
Third Party Applications

- **Fool Proof**
  - Locks access to start menu, command shell, etc.

- **Fortes 101**
  - [http://www.fortres.com](http://www.fortres.com)
  - Locks access to start menu, command shell, etc.
Third Party Applications

- **Foolproof**
  - Provided little info on their website
  - Allowed download of demo
  - Must call company to get an unlock code

- **Fortres**
  - More information on their website
  - Allowed download of demo
  - Must call or fax company to get an unlock code
Third Party Applications

- FoolProof is a GREAT program! It's very flexible and easy to use and you don't even know it's there! It has saved me countless hours by preventing students from renaming/trashing files; moving things around so that they can't be found; changing settings; and all-in-all not causing more work or damage! 

—Karen Golubic, Computer Coordinator, Girard, PA
Third Party Applications
There is no such thing as security

- All methods discussed have flaws and can be circumvented.

Fortres, for instance, displays a code in the window title of the password entry box. This can be used to get the backdoor password.
Backdoor Password

unsigned short backdoor_password( unsigned long key )
{
    short x;

    x = ((short)( key * -1.2456 ) + 1 ) * 65533;
    x = ( x / 2 + 7 ) * 3;
    x /= 2;
    return x * x;
}
Conclusion

No method of locking down the Windows box is perfect. All methods have flaws and can be bypassed. Using combinations of methods, such as third party applications in conjunction with a guest account and some registry tweaking will prevent the average hoodlum from creating more work for you.