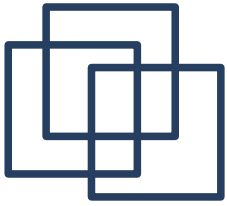


Portable Applications

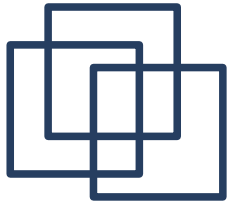
Presentation about the pros and cons of portable applications and how to deal with them.

Presentation of 02/02/2009
for HCC-VI : Mechelen



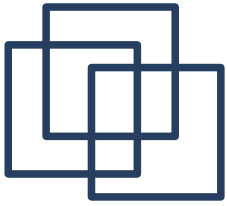
Content

- What is a „Portable Application“
- Types of portable applications
- Dealing with portable applications



Content

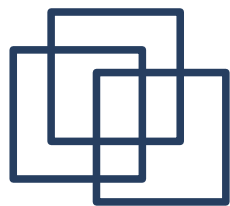
- What is a „Portable Application“
 - Definition
 - Advantages
 - Disadvantages
 - Risks
- Types of portable applications
- Dealing with portable applications



Definition

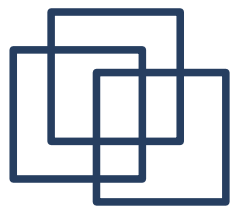
- Wikipedia

„A portable application is a computer software program that runs from a removable storage device such as a CD-ROM drive, USB flash drive, flash card or floppy disk“



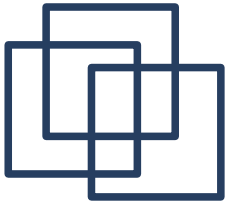
Advantages

- Take it with you
- No administrator rights needed
- No cluttering of registry, startup menu, desktop icons, ...
- Easy maintenance for larger networks



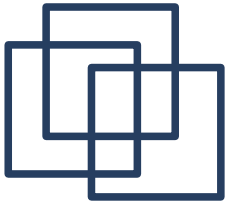
Disadvantages

- Consumes more disk space
- Security updates (third party delivery)
- Not (or less) integrated with environment



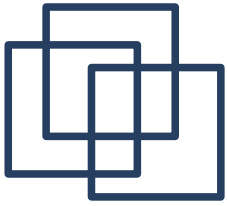
Risks (1)

- Licensing
- Stability (Operating System)
- Security
 - Security updates
 - Features you do not want to allow
 - Information leakage



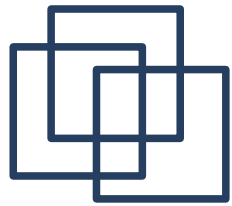
Risks (2)

- Process control
 - If become part of logical chain
 - Monitoring
- Juridical consequences



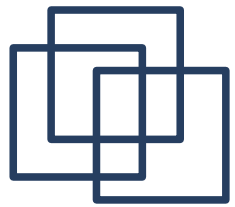
Content

- What is a „Portable Application“
- Types of portable applications
 - Stand-alone applications
 - Modified stand-alone applications
 - Intermediate layer
 - Using emulation / virtualization
- Dealing with portable applications



Stand-Alone Apps

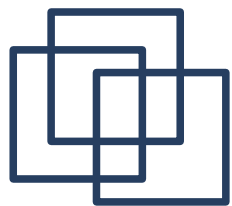
- Applications that are developed to be runnable without further installation requirements
- Many on <http://www.pendriveapps.com> and <http://appstogo.mcfadzean.org.uk/>



Modified Applications

- Applications that are modified and/or repackaged to be runnable without further installation requirements
- Two types of „portability“
 - Use host resources but clean afterwards
 - Do not use host resources

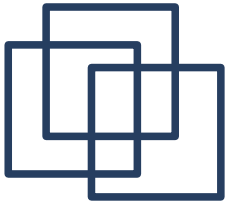
Line is beginning to fade though...



Use host resources

(Modified Applications)

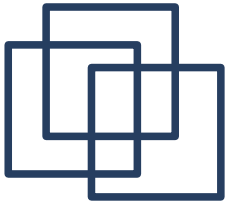
- Modified or repackaged software
- Either require host resource (software)...
- ... or use host resource (registry, disk, ...)
- Luckily,
 - Required software without admin-rights
 - Registry access without admin-rights
 - Disk access without admin-rights



U3

(Modified Applications)

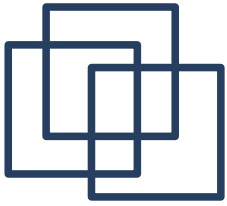
- <http://www.u3.com>
- Can use OS resources (registry, ...)
- Removes traces when shut down
- Includes off-the-shelf software
- Lots of criticism (instability, closed API)



Klik

(Intermediate layer)

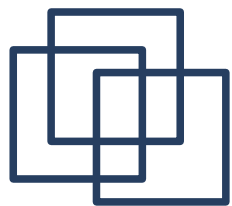
- <http://klik.atekon.de/>
- Features
 - One file, one application
 - Simple „recipe“ generates image
 - Driven by links (klik://...)
- Well supported (packages++)



Oinstall

(Intermediate layer)

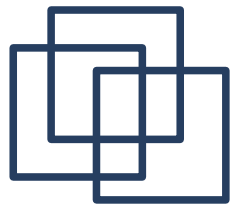
- <http://Oinstall.net>
- Features
 - Dependency support
 - Automatic upgrading
 - Shared libraries
 - Shared downloads



Do not use host res.

(Modified Applications)

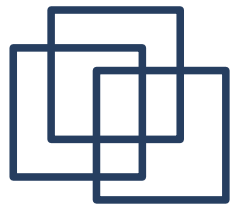
- Real „portable applications“
- Still requires Operating System
- Many different implementations
 - Use specific resource wrapper, or
 - Repackaged for standalone running
- Examples follow...



PortableApps.com (1)

(Modified Applications)

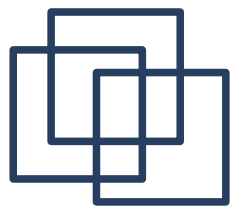
- Repackaged for stand-alone use
- <http://www.portableapps.com>
- Almost only free software
- Uses NSIS for special installation
- Uses common API for all applications
 - Recent development: also OS changes



PortableApps.com (2)

(Modified Applications)

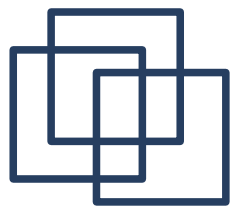
- Offers single-download suites
 - Suite Light
 - Suite Standard (Light + OpenOffice)
- Similar project is AccessApps
<http://www.rsc-ne-scotland.ac.uk/accessapps/>



Sphinx Software

(Modified Applications)

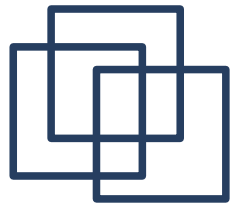
- Company that delivers portable apps
- Support for off-the-shelf applications
- Probably expensive too...
- <http://sphinx-soft.com/Portable>



JauntePE

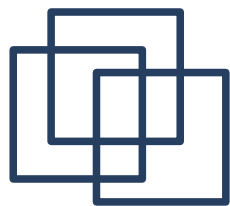
(Modified Applications)

- <http://www.box.net/shared/4cx4i2k00r>
- Framework for DIY portable-making
- Example for Putty:
<http://portablefreeware.com/forums/viewtopic.php?t=1542&start=45>
- Full HOWTO:
<http://portablefreeware.com/forums/viewtopic.php?t=2182>



Intermediate Layer

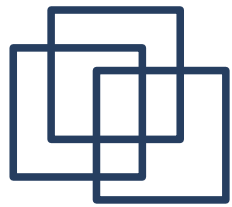
- Requires framework software
- Examples are well-known
 - Java
 - .NET
 - Firefox



Java (1)

(Intermediate Layer)

- webstart
- Example applications
 - JPC (Virtualization software for x86)
<http://www-jpc.physics.ox.ac.uk/>
 - NetBeans (IDE)
<http://www.netbeans.org/>
 - JBoss (Application Server)
<http://jboss.org/>



Java (2)

(Intermediate Layer)

- Directories

- Freshmeat

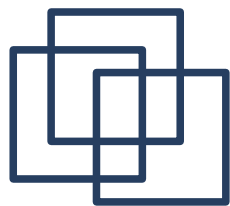
- <http://freshmeat.net/browse/198>

- JavaBoutique

- <http://javaboutique.internet.com>

- java.dev

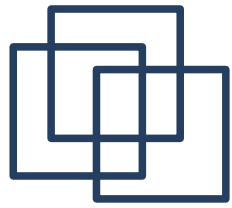
- <http://dev.java.net>



Firefox

(Intermediate Layer)

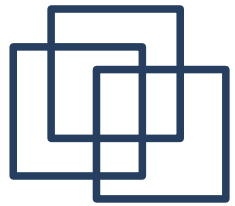
- Powerful extensions support
- Examples
 - Meebo (IM)
 - Cooliris (Image navigation)
 - CaptureFOX (Screen capture)



Scripting Languages

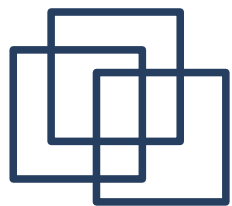
(Intermediate Layer)

- Perl, Python, Tcl/tk, Ruby, ...
- Difficult to counter if language required (but not impossible)



Emulation and higher

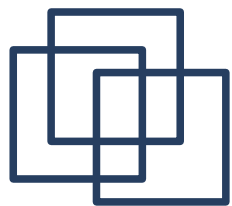
- Emulate operating system, or
- Virtualize operating system
- Small requirement:
 - Emulation / virtualization software should be stand-alone
- „Portable“ VMWare



VMWare's ThinApp

(Emulation and higher)

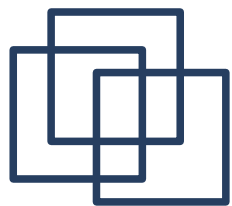
- <http://www.vmware.com/products/thinapp>
- Shell surrounding syscalls, ...
- Based upon VMWare's virtualization
- Quite expensive (€ 5000 for non-academic use)



MojoPAC

(Emulation and higher)

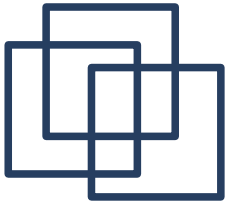
- <http://www.mojopac.com>
- Virtual Windows environment
 - Reuses host Windows files though
- Requires administrator-rights, but
- Limited user version is being developed



Ceedo Personal

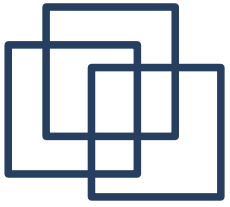
(Emulation and higher)

- <http://www.ceedo.com>
- Implements virtualization layer
- Does not implement full virtualization
 - Host OS is still used
 - Specific installer needed



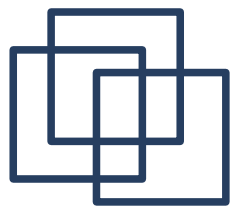
Content

- What is a „Portable Application“
- Types of portable applications
- Dealing with portable applications
 - Supporting portable applications
 - Explicitly denying portable applications



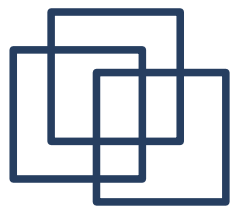
Supporting PA

- Mitigate the risks
- Implement policy for use of PA
- Deny PA you do not want to support



Denying PA

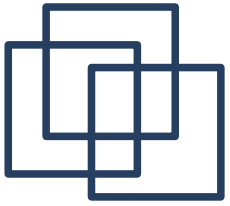
- Various technologies exist
- Hash rules
- Certificates
- Paths
- Zones
- MAC



Hash rules

(Denying PA)

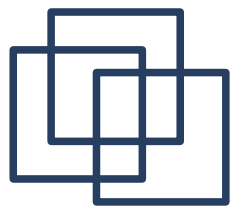
- Only run software whose hash matches
- Supported by Microsoft's Software Restrictions Policy (SRP)
<http://technet.microsoft.com/en-us/library/bb457006.aspx>



Certificates

(Denying PA)

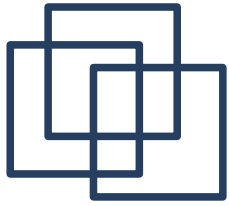
- Only run signed and trusted software
- Supported by Microsoft's SRP
- Supported by DigSig for Linux
<http://disec.sf.net>
- Supported by Java VM (by design)
- Support on the way for scripting languages



Paths

(Denying PA)

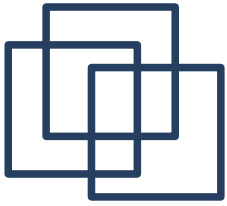
- Disallow based on location (file system)
- Supported by Microsoft's SRP
- Supported by NTP QFS
<http://www.ntp.com>
- Supported by Trust-No-Exe
<http://www.beyondlogic.org>
- Supported by Linux/Unix (noexec)



Zones

(Denying PA)

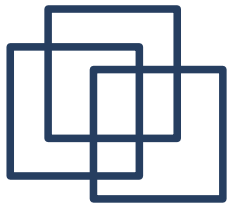
- Disallow based on origin (Internet/...)
- Less operating system specific
- More for applications
 - Browsers (ActiveX, Java, ...)
 - Microsoft Office (Macro's)
 - ...



MAC

(Denying PA)

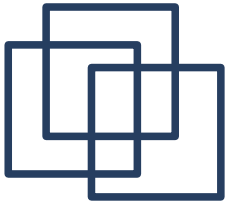
- Mandatory Access Control
- „Security as it should be“ (?)
- Complete security implementation, including
 - Who can run what software when
 - Which software can be run
 - What privileges should be used



SELinux

(Denying PA - MAC)

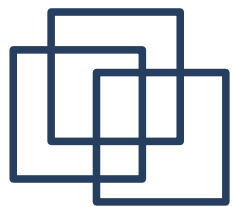
- <http://selinuxproject.org>
- MAC implementation for Linux (LSM)
- Well supported by most major distributions
- Has file system requirements
- Can be difficult to administer at first



RSBAC

(Denying PA - MAC)

- <http://www.rsbac.org>
- Similar features to SELinux, but
 - Easier to implement (subjective)
 - Not in Linux by default



Questions?

