

Preserving Privacy with Virtual Machines

Saturday, April 2, 2011

Sunday, April 3, 2011

Trenton Computer Festival
College of New Jersey
Ewing, New Jersey

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
<http://www.rlgsc.com>

If it makes a sound, SET IT ON SILENT
(e.g., mobiles, pagers, PDA, smartphone)

Many privacy threats –

- visitor tracking has become ubiquitous
- malware
- spyware
- persistent threats

Many mechanisms involved:

- cookies
- Registry
- spyware
- ActiveX
- others

Browsers are somewhat “sandboxed”

- “sandboxes” are not always perfect
- force vendoris/demandus
- employers
- “must use” applications

The problem:

- Compromise is not inevitable
- There are solutions

The solution:

- turn the paradigm on its head
- use a VM with “differencing” disks
- dispose of the system afterwards

After the visit:

- Delete the “difference” disk
- no preserved information

Demonstration:

- Create and use a “disposable” system
- Tasks:
 - Base System: Windows XP SP2
 - Create profile
 - Create new “difference” disk

Using Test System

- Browse a few www sites

Perform Teardown

- halt virtual system
- delete “difference” disk
- create new “difference” disk
- boot disposable system
 - check history
 - browse location

Summary

- privacy can be preserved using disposable VMs
- that which is erased is not preserved

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
<http://www.rlgsc.com>

Session Notes & Materials:

<http://www.rlgsc.com/trentoncomputerfestival/2011/index.html>