Microsoft’s Security Perspective and Collaboration

Andrea Valboni
National Technology Officer
Public Sector
Microsoft Italy
Evolving Security Threat Landscape

Trustworthy Computing Vision

Addressing Security Threats

Public Private Partnership
THREAT LANDSCAPE

Where are threats heading next?
<table>
<thead>
<tr>
<th>Alert and prescriptive guidance</th>
<th><strong>Blaster</strong></th>
<th><strong>Sasser</strong></th>
<th><strong>Zotob</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Within 1 day</td>
<td>Within 2 hours</td>
<td>2 days prior</td>
</tr>
<tr>
<td>Online guidance/ Web cast</td>
<td>Within 10 days</td>
<td>Within 2 days</td>
<td>Same day</td>
</tr>
<tr>
<td>Free worm removal tool</td>
<td>Within 38 days</td>
<td>Within 3 days</td>
<td>Within 3 days</td>
</tr>
<tr>
<td>Arrests made</td>
<td>Within 7 days</td>
<td>Within 11 days</td>
<td></td>
</tr>
</tbody>
</table>
Top Security Challenges

Virus and Malware Prevention
- Viruses, Spyware and Worms
- Botnets and Rootkits
- Phishing and Fraud

Business Practices
- Regulatory Compliance
- Development & Implementation Security Policies
- Reporting and Accountability

Implementing Defense in Depth
- Identity Management and Access Control
- Managing Remote Access
- Security Risk of Unmanaged PCs

Security Management
- Deploying Security Updates
- System Identification and Configuration
- Security Policy Enforcement
Local Area Networks
First PC virus
Boot sector viruses
Create notoriety or cause havoc
Slow propagation
16-bit DOS

Internet Era
Macro viruses
Script viruses
Create notoriety or cause havoc
Faster propagation
32-bit Windows

Broadband prevalent
Spyware, Spam
Phishing
Botnets
Rootkits
Financial motivation
Internet wide impact
32-bit Windows

Hyper jacking
Peer to Peer
Social engineering
Application attacks
Financial motivation
Targeted attacks
64-bit Windows

1986-1995
1995-2000
2000-2005
2006-2007
Exponential Growth of IDs
Identity and access management challenging

Increasingly Sophisticated Malware
Anti-malware alone is not sufficient

National Interest
Personal Gain
Personal Fame
Curiosity

Crime On The Rise

Attacks Getting More Sophisticated
Traditional defenses are inadequate

Number of Digital IDs

Internet

mobiility

B2B
B2C

Pre-1980s 1980s 1990s 2000s

Largest area by volume

Largest segment by $ spent on defense

Fastest growing segment

National Interest
Personal Gain
Personal Fame
Curiosity

Script-Kiddy
Amateur
Expert
Specialist

User
GUI
Applications
Drivers
O/S
Hardware
Physical

Examples
- Spyware
- Rootkits
- Application attacks
- Phishing/Social engineering

Source: Microsoft Security Intelligence Report (January – June 2007)
Major sections cover
- Software Vulnerability Disclosures
- Software Vulnerability Exploits
- Malicious Software and Potentially Unwanted Software
- Privacy and Security Breach Notifications

www.microsoft.com/sir
Malicious Software and Potentially Unwanted Software

- Data from several hundred million computers
- MSRT has a user base of 450+ million unique computers
- During 2H07 MSRT executed 2.5 billion times
- Since January 2005 total MSRT executions surpass 10 billion
More than 2,700 new vulnerabilities disclosed in 2H07
2H07 had the lowest number of disclosures since 2H05
Total vulnerabilities for 2007 lower than 2006
900 security breach notifications, 12 countries
Exploits, malware and hacking less than 23 percent of all notifications from 2000 - 2007, only 13 percent during 2H07
Breaches in 2H07 involved proportionally fewer hacking incidents than the last eight years as a whole
57% of breaches in 2H07 resulted from lost or stolen equipment

Data sourced from the Data Loss Database at http://attrition.org/dataloss
Malicious Software
Top 5 Categories in Italy

2007

- Trojan Downloader: 30.27%
- Trojan: 29.06%
- Backdoor: 21.12%
- Worm: 11.49%
- Exploit: 8.06%
PLATFORM FOR SECURITY

Trustworthy Computing Vision
Secure against attacks
Protects confidentiality, integrity and availability of data and systems

Microsoft Security Response Center (MSRC)
Microsoft Malware Protection Center (MMPC)
Secure Windows Initiative (SWI)

Build solutions that protect privacy
Safe guard your corporate data
Protect Personal Privacy

Microsoft Online Crash Analysis
Engineering Excellence Training and Guidelines
Microsoft Online Services with high reliability in multiple data centers
Vendor Engagement and Windows Hardware Quality Lab
Business Continuity explicitly designed in with prescriptive guidance
Interop Vendor Alliance
Open Source Software Lab
Transparent Practices (SDL, Codeplex, etc.)

Microsoft Privacy Guidelines for developing Software and Services
Microsoft Data Governance Framework
Managing and Protecting Personal Information

Predictable, consistent, responsive service, consistent, responsive service, consistent, responsive service
Maintainable, easy to configure and manage, easy to configure and manage, easy to configure and manage
Resilient, works despite changes, works despite changes, works despite changes
Recoverable, easily restored, easily restored, easily restored, easily restored
Proven, ready to operate, ready to operate, ready to operate

Commitment to customer-centric interoperability
Automated Policy-Based Solution set (MPC)
Recognized industry leader, world-class partner
Open, transparent

SQL Server 2005
Visual Studio 2005
Windows Server 2003 SP1
Malicious SW Removal Tool
Windows Defender
Windows Live OneCare
Windows Vista
Office 2007
Forefront

Windows Server 2008
SQL Server 2008

2002
2003
2004
2005
2006
2007
2008

TWC Announced
SDL begins
Windows Server 2003
Windows XP SP2, DSI Launched
SQL Server 2005
Visual Studio 2005
Windows Server 2003 SP1
Malicious SW Removal Tool
Windows Defender
Windows Live OneCare
Windows Vista
Office 2007
Forefront
Windows Server 2008
SQL Server 2008

2002
2003
2004
2005
2006
2007
2008
The Microsoft Security Development Lifecycle

**Goals**
- Protect Microsoft customers by
  - Reducing the *number* of vulnerabilities
  - Reducing the *severity* of vulnerabilities

**Key Principles**
- Prescriptive yet practical approach
- Proactive - not just “looking for bugs”
- Eliminate security problems early
- Secure by design
At Microsoft, we believe that delivering secure software requires:

Executive commitment → SDL a mandatory policy at Microsoft since 2004

Ongoing Process Improvements → 6 month cycle

**Embedding Security Into Software And Culture**

Core training
- Analyze security and privacy risk
- Define quality gates

Education

Requirements
- Threat modeling
- Attack surface analysis

Design
- Specify tools
- Enforce banned functions
- Static analysis

Implementation
- Dynamic/Fuzz testing
- Verify threat models/attack surface

Verification
- Response plan
- Final security review
- Release archive

Release
- Response execution

Response
First Year of Vulnerabilities

2007

Vulnerabilities Fixed One Year After Release

Quarterly totals, 2000-2006


Source: http://blogs.csoonline.com/blog/jeff_jones

SDL Results

Windows XP

Fixed  Unfixed

65  30

Windows Vista

54  36

Windows XP SP2

5  15

Windows Vista

35  19

IE 6

18  3

IE 7

14  3

Vulnerabilities disclosed and fixed

Microsoft SQL Server

Critical  Important  Moderate  Low

2  4

7  17

*Source: http://blogs.csoonline.com/blog/jeff_jones

**Source. Which database is more secure? Oracle vs. Microsoft, David Litchfield, NGS Software, 21-November-2006
Addressing Security Threads
Policy, People, Processes (and Technology)
### Core Infrastructure Optimization Model

**Leverage IO to understand your security infrastructure**

<table>
<thead>
<tr>
<th>Basic</th>
<th>Standardized</th>
<th>Rationalized</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>No common identity management model</td>
<td><strong>Identity and Access Management</strong></td>
<td>Federated Identity Management across org. and platform boundaries</td>
<td></td>
</tr>
<tr>
<td>No desktop or server standards, many images, no management standards</td>
<td><strong>Desktop, Device and Server Management</strong></td>
<td>Automated IT management, dynamic resource usage</td>
<td></td>
</tr>
<tr>
<td>No networks and security standards</td>
<td><strong>Security and Networking</strong></td>
<td>Automated security and network management</td>
<td></td>
</tr>
<tr>
<td>Adhoc protection of key data</td>
<td><strong>Data Protection and Recovery</strong></td>
<td>End to end data protection and disaster recovery</td>
<td></td>
</tr>
<tr>
<td>Adhoc, reactive</td>
<td><strong>IT and Security Process</strong></td>
<td>Proactive, Optimize cost &amp; quality, End-to-End service &amp; policy management</td>
<td></td>
</tr>
</tbody>
</table>
Building A Trusted Stack

Core Security Components

- Identity Claims
- Authentication
- Authorization
- Access Control Mechanisms
- Audit

Trusted Stack

- Trusted Data
- Trusted People
- Trusted Software
- Trusted Hardware

Secure Foundation

Integrated Protection

- SDL and SD3
- Defense in Depth
- Threat Mitigation
End To End Trust

Economic Forces

Social Requirements

Core Security Components
- Identity Claims
- Authentication
- Authorization
- Access Control Mechanisms
- Audit

“1+4A”

Trusted Stack
- Trusted Data
- Trusted People
- Trusted Software
- Trusted Hardware

Secure Foundation

Integrated Protection
- SDL and SD3
- Defense in Depth
- Threat Mitigation
Microsoft Security: Defense In Depth

A well Managed Secure Infrastructure is the key!
Public Private Partnerships

Initiatives in Italy during 2007
“La scuola ricomincia navigando” (School starts again …. Surfing)
A pilot project for a single local municipality (Comune di Roma) with the following format:

- The Rome municipality send mail with project presentation to all the schools managers in Rome (kids aged 11-13) proposing them
  1. One day of Classroom lessons by the local law enforcement agency (Polizia Postale e delle Comunicazioni) for all the students and the teachers using the Get Net Safe deck for presentation
  2. Specific teacher training (Partner in Learning train the trainer with Microsoft security curricula) and resources to create classroom lessons
  3. A contest for all the classroom involved (video production)
  4. Materials for kids and parents to be distributed to all the participants

<table>
<thead>
<tr>
<th></th>
<th>Results FY07</th>
<th>Target FY08</th>
<th>Forecast FY08</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kids direct Touches</td>
<td>10,000</td>
<td>20,000</td>
<td>29,800</td>
</tr>
<tr>
<td>Schools direct Touches</td>
<td>46</td>
<td>70</td>
<td>92</td>
</tr>
<tr>
<td>Teachers direct Touches</td>
<td>500</td>
<td>1,000</td>
<td>1,526</td>
</tr>
<tr>
<td>Government elites direct touches</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>Top Stories</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Family Safety registered parents</td>
<td>3,500</td>
<td>3,500</td>
<td>50,000</td>
</tr>
<tr>
<td>Family Safety registered children</td>
<td>700</td>
<td>3,500</td>
<td>5,000</td>
</tr>
</tbody>
</table>
Child Exploitation Tracking System is a unique software tool that helps protect children from exploitation online. It enables more effective identification and prosecution of offenders by allowing governments to store, search, share, and analyze evidence in child exploitation cases across police agencies.

As of June 2007, the Child Exploitation Tracking System has been deployed in seven countries and is being used by over 400 investigators worldwide. With it, law enforcement agencies can break down borders through collaboration and information sharing.

Polizia Postale is the Italian Partner for this world wide program.
Computer Online Forensic Evidence Extractor (COFEE)

- Not to cause unnecessary input to the target machine
- Collect the volatile data including network, and memory information for investigation
- Documentation of execution flow for court presentation
- Backup passwords from the machine for future forensic purpose

**Reconnaissance**

**Digital Forensics**

**Relevancy**

**Reliability**
Security Cooperation Program

- Designed to help government CERT in defending critical infrastructure in the PA space from IT threats, through advanced information sharing on MS security bulletins, workshops and training.

Ad hoc local programs to address unique requirements for a given Country

- Might include the creation of competence centers on IT security, citizen’s security initiative, Public Protection.
Microsoft Security Home Page:  www.microsoft.com/security
www.microsoft.com/italy/security
Microsoft Trustworthy Computing:  www.microsoft.com/security/twc
Microsoft Forefront:  www.microsoft.com/forefront
Infrastructure Optimization:  www.microsoft.com/io
Microsoft Security Assessment Tool:  www.microsoft.com/security/msat

General Information:
Microsoft Live Safety Center:  safety.live.com
Microsoft Security Response Center:  www.microsoft.com/security/msrc
Security Development Lifecycle:  msdn.microsoft.com/security/sdl
Get the Facts on Windows and Linux:  www.microsoft.com/windowsserver/compare

Anti-Malware:
Microsoft OneCare Live:  beta.windowsonecare.com
Microsoft Defender:  www.microsoft.com/athome/security/spyware/software
Spyware Criteria:  www.microsoft.com/athome/security/spyware/software/isv

Guidance Centers:
The Microsoft Security Developer Center:  msdn.microsoft.com/security
The Security at Home Consumer Site:  www.microsoft.com/athome/security
Windows Vista - First 12 Months

First Year of Vulnerabilities

<table>
<thead>
<tr>
<th>Metric</th>
<th>Windows Vista (year 1)</th>
<th>Windows XP (year 1)</th>
<th>Red Hat rhel4ws reduced (year 1)</th>
<th>Ubuntu 6.06 LTS reduced</th>
<th>Mac OS X 10.4 (year 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities fixed</td>
<td>36</td>
<td>65</td>
<td>360</td>
<td>224</td>
<td>116</td>
</tr>
<tr>
<td>Security Updates</td>
<td>17</td>
<td>30</td>
<td>125</td>
<td>80</td>
<td>17</td>
</tr>
<tr>
<td>Patch Events</td>
<td>9</td>
<td>26</td>
<td>64</td>
<td>65</td>
<td>17</td>
</tr>
<tr>
<td>Weeks with at least 1 Patch Event</td>
<td>9</td>
<td>25</td>
<td>44</td>
<td>39</td>
<td>15</td>
</tr>
</tbody>
</table>

http://blogs.csoonline.com/blog/jeff_jones
Windows Vista in 2007

- 20% fewer vulnerabilities than Windows XP
- 74% fewer vulnerabilities than the next closest (Ubuntu)
- 47% fewer high severity vulnerabilities than the next closest (Red Hat)

Source: http://blogs.csoonline.com/blog/jeff_jones