A real world look at practical implementation issues and solutions of Intrusion Prevention

Ralph Harvey
Chief Technology Officer, Prevx Inc
December 9th 2004
Agenda

► Motivation
► Terminology
► Challenges
► Case Study: Our Solution
► Summary
Motivation

► Fight Cyber-Crime and Make Money 😊
► Current forms of protection alone are not generally effective
What is Intrusion Prevention Software?

► For this case study, Intrusion Prevention Software refers to:
  ► PREVENTION of intrusion of zero day and non-zero day threats
  ► Non-signature centric
  ► Protects system resources via policies/rules
  ► Records rule violations via ‘events’
  ► For practical purposes – it needs to be manageable

There is no accepted single industry standard definition for IPS today!
What is a policy?

- Buffer Overflow Protection
- Process Hijack Protection
- Memory Protection
- Network Protection
- Registry Protection
- File System Protection
- Centralised Exception Lists
- Local User Exception Lists (optional)
- pre-shipped Exception Lists

- NON-EXEC D IR P R O T E C T I O N

- FTP
Challenges for Intrusion Prevention Technology

- False Positives (noise)
- False Negatives
- Usability
- Defining Policies/Rules
- Managing Policies/Rules
- Collating, Reporting, analyzing on Data
- Cost of Ownership
- Performance
- Scalability
- Sabotage and Subterfuge
Challenges: A real world trade off …..

► Implementing secure systems is a matter of compromise.
► The more you compromise the more you are compromised.
► The less you compromise the less viable the solution becomes.

► We realised we didn’t have all the answers, but we had more than anybody else.
► The only way to gain a holistic insight was to hunt in packs. Expertise was obtained by unique heuristics approach to IPS.
Case Study: The Prevx Solution

- Provide a Scalable back end database technology
- Implement a Kernel Device Driver
- Provide a user interface for the desktop
- Provide a web based administration interface
- Provide a web based reporting and query interface
- Provide a DNA architecture for threat events
- Implement a white list scheme
- Implement realtime ‘get advice’ assistance
- Allow the IPS system to ‘hunt in packs’
Agent User Interface – Main Screen

Agent User Interface – Main Screen

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system.

98% Protection Level

Click on a prong for more information about the types of attack that Prevx Home stops.

Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

Prevx Pro's unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact: pro-support@prevx.com
Agent User Interface – Security Settings

Prevx Pro Management Console

Settings
- Physical Memory Overwrite
- BAT Files in Download Areas
- BAT Files in Program Areas
- BAT Files in System Areas
- CMD Files in Download Areas
- CMD Files in Program Areas
- CMD Files in System Areas
- COM Files in Download Areas
- COM Files in Program Areas
- COM Files in System Areas
- CPL Files in Download Areas
- CPL Files in Program Areas
- CPL Files in System Areas
- DLL Files in Download Areas

Install Attempt (.bat)
Prevents files named *.bat in the Downloaded Program Files directory (and its subdirectories) from being created or modified. Worms, trojans and malware often use these directories.

Protection Level
- User Defined

You can prevent, query, report or turn off security settings. Select QUERY if you want to be prompted to allow or deny an Event.

Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

Prevx Pro’s unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact: pro-support@prevx.com
The Agent User Interface – Event History
Agent User Interface - Preferences

Prevx Pro - Management Console

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from Internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system.

Protection Level: 98%

Update every:
- 30 Day(s)
- 10 Events

Clear history if more than:
- 10 Events

- be part of the Prevx Advanced Warning System
  "Paws Insight" gives you a unique insight into the live Threat-Data collected by the Prevx PAW-System.

- Enable password protection
- Password required for Query Operations

Rules Management:
- "Don’t notify me again" rules
- Advanced options for Queries

Protection Level:
- User Defined

Save Changes

Protect your configuration from unauthorized changes by setting a password.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

Prevx Pro’s unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact:
pro-support@prevx.com
Agent User Interface – Editing Rules

The Rule Editor is used to manage user defined rules. Note: These rules only apply to security settings that have been set to Query mode.

Right-click on an item for more options.

Item information
Event Pop UP

**Prevx Event**

**File System Event**

**POTENTIAL INTRUSION ATTEMPT DETECTED**

**Summary**

The application `NTVDM.EXE` is trying to **READ, WRITE** the protected file/directory `C:\WINDOWS\FRED.EXE`

**Install Attempt (*.exe)**

This is due to a program trying to modify a protected file or directory. Windows updates and software installations/configurations may modify these files. If you are not installing or updating any programs, then this may be malicious activity.

Event 1 of 1

- **Event Details**
- **Terminate**
- **Get Advice**
- **Suspend**

- **Remember my answer for ONLY the application shown above:**
- **Allow**
- **Deny**
IPS Case Study: Policy Definition via XML (raw view)

- Meta Policy Data ================

  Title: MS Installer (Installing Attempt)
  Key: /
  Version: 00.0
  Platform: Windows
  Security Type: Registry
  Attributes: Queryable, Reportable, Mutable
  Install Mode: Mandatory
  Default: query
  Policy ID: 0100103000

- <policy ID="0100103000" inherit="all">
  - <process>
    <name />
    <platform>Windows</platform>
  </process>
  - <image> <!-- All executables -->
    <path>\.*</path>
    <excludedPath>%ProgramFiles%\PREVX\.*\PXL1.exe</excludedPath>
    <excludedPath>$$PREVX:Reg:PREVXHome\.*\PXL1.exe</excludedPath> <!-- Windows Update Applications -->
    <excludedPath>%SystemRoot%\System32\wuauclt*.exe</excludedPath>
    <excludedPath>WUTemp\com_microsoft.*\*.exe</excludedPath> <!-- Microsoft Management Console -->
    <excludedPath>%SystemRoot%\system32\mmc.exe</excludedPath>
    <excludedPath>%WinDir%\system32\mmc.exe</excludedPath> <!-- Exclude the following Anti-Virus tools: -->
    <excludedPath>%ProgramFiles%\PREVX\.*\PXL1.exe</excludedPath>
    <excludedPath>$$PREVX:Reg:PREVXHome\.*\PXL1.exe</excludedPath>
  </image>

--

- Exclude the following Anti-Virus tools:
  - Kaspersky

--
Managing Data: Prevx Advanced Warning
Top threat monitoring
Coolwebsearch attack
Drilling Down into events – company reports
Policy Management and Tracking
Policy Violations Monitoring

![Graph showing total violations for all policies by operating system between Dec 7 2004 00:00 and Dec 8 2004 00:00.]
Tracking Events

Events By Day

- Y-axis: 0 to 350,000
- Data points for each day showing event count
Intrusion Prevention – Case Study Summary

- Prevx have implemented a product and expertise based solution that is working for > 250,000 active users today
- The techniques and software adopted can be applied to both controlling and monitoring access to key resources as well as pure Intrusion Prevention
- The product and knowledge based architecture scale from consumer (free) versions through to Enterprise implementations.

- Try it for free at www.prevx.com
QUESTIONS?

Ralph Harvey
CTO Prevx Inc
ralph.harvey@prevx.com
www.prevx.com