Principled Technologies®

WHITE PAPER
August 2007

Options for reducing intrusion security risks

Enterprises seeking to reduce security costs are considering multiple computing models available today. This Intel®-commissioned white paper examines two current models—Intel® vPro™ processor technology and Intel® Centrino™ Pro processor technology clients and server-based computing—that can help achieve this goal. We pay particular attention to the computer crime categories that account for the majority of security-related financial losses. We restrict our scope to intrusion security: creating a more secure environment while not intruding on the work of authorized users. For more information on the related topic of data security, protecting data users are accessing, see our white paper "Rich clients with thin client security: a hybrid approach."

Eight categories account for over 90 percent of financial losses

1. Virus contamination/malware (29.89 percent)
2. Unauthorized access to information (20.23 percent)
3. Notebook or mobile hardware theft (12.65 percent)
4. Theft of proprietary information (11.49 percent)
5. Denial of service (DoS) (5.57 percent)
6. Financial fraud (4.87 percent)
7. Insider abuse of net access/e-mail (3.52 percent)
8. Telecom fraud (2.40 percent)

(Source: CSI/FBI Computer Crime and Security Survey.)

In this paper, we address Categories 1 to 5, for which the security risks differ depending on the computing model. Categories 6 to 8 involve individuals misleading others or misusing their legitimate resources and privileges; because no computing model can distinguish between misuse and legitimate use, this white paper will not cover these topics. For more detail on the eight categories and how we defined them, see Appendix A.

How this costs corporations

- Average percentage of PCs infected each month: 11.
- Average server downtime during a virus disaster (25 or more PCs or servers infected): 23 hours.
- Average cost to recover from a single virus disaster: $130,000+.

(Source: ICSA Labs' Tenth Annual Virus Prevalence Survey.)

How Intel® vPro™ processor technology and Intel® Centrino™ Pro processor technology address security problems

The hardware-based capabilities of Intel® vPro™ processor technology and Intel® Centrino™ Pro processor technology, coupled with appropriate remote management and related third-party software products, enable IT departments to filter threats and isolate PCs, verify and improve the reliability of security agents, and improve the distribution of security software. To achieve many of these benefits, IT must, of course, have strict policies in place.

- Hardware and software filters let you inspect both inbound and outbound traffic for malware. Third-party management tools let you add application-defined filters to the standard Intel® vPro™ processor technology filters. These filters compare five data points against preset rules: source IP address, destination IP address, source port number, destination port number, and protocol type. Filtering occurs regardless of the state of the operating system or virus-protection agents.
- Third-party management tools can use Agent Presence to insure that anti-virus software is running. Agent Presence software polls for the presence of management and security software via the Intel® Active Management Technology (AMT) firmware and requires the following capabilities from third-party applications:
    - ability to register with the Intel® AMT Agent Presence Monitor

    - ability of configuration management applications to recognize Intel® AMT alerts
- Third-party management tools let you use hardware-based Intel® Virtualization Technology to increase security of virtualized applications. This hardware-based memory protection feature keeps processor-state information for each Virtual Machine Manager (VMM) and each guest operating system in dedicated address spaces and can create “virtual appliances,” self-contained operating environments each of which you can dedicate to a particular function, such as security checking.
- Third-party management tools can use System Defense to automatically quarantine an infected PC. Triggered by Agent Presence or network filters, System Defense can automatically quarantine and repair an infected PC. It requires a third-party management console capable of defining Inspect and Repair System Defense policies.
- Secure Management Engine memory lets you keep encryption keys and other configuration data safe. Nonvolatile memory holds the following:
    - storage for the signed, encrypted Intel® Management Engine and other information Intel® AMT uses
    - storage for hardware asset information, BIOS configuration information, the unique ID, the event log, and other system information
    - the 3PDS (third-party data store), storage authorized IT administrators can configure for third-party software use
- Hard disk encryption technologies from third parties, such as Microsoft Windows Vista BitLocker, help keep local data safe. These technologies protect user and system data even if someone tampers with the PC when the OS is offline. BitLocker uses the Trusted Platform Module features in Intel® vPro™ processor technology technology.

How server-based computing addresses security problems

Server-based computing does not so much offer features that boost security as it lacks features that can create security vulnerabilities.

- Thin client devices lack local storage and have only minimal operating systems, so they are very difficult to infect.
- Thin client devices are useless unless connected to the network. A network disruption consequently stops all work, and users lose any work in progress.
- The limitations of these client devices also provide some security advantages:
    - Being inexpensive and of limited usefulness make them minimally interesting to thieves.
    - By having no local storage and minimal local software, they leave little vulnerable to attack.
- Any application or operating system patch to a server immediately applies to all clients on that server.

Sources of financial loss: Eight categories account for over 90 percent of losses

Source: CSI/FBI Computer Crime and Security Survey 2006

	Intel® vPro™ processor technology and Intel® Centrino™ Pro processor technology	Server-based computing with thin clients
1. Virus contamination/malware (29.89 percent) Includes viruses, worms, Trojans, adware, spyware, rootkits, loggers, botnets, etc.		
Vulnerability to attack	● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools to configure security software to run virtualized in a "security appliance." ● Intel® vPro™ processor technology-enabled third-party management tools using System Defense automatically isolate infected systems. ● Local storage can harbor viruses.	● A virus attack that brings down a server will also bring down all the thin client users working on that server.
Window of vulnerability	● Intel® vPro™ processor technology-enabled third-party management tools using network filters can quickly detect suspicious behavior. ● Intel® vPro™ processor technology-enabled third-party management tools using Agent Presence can ensure Anti-virus software is running. ● IT managers using Remote Power-on and Intel® AMT via Intel® vPro™ processor technology-enabled third-party management tools can heal infected systems, even if users have powered off those systems or the OS is down.	● Any patch to a server immediately applies to all clients on the server.
Effects of contamination	● Users can work locally if server is unavailable. ● IT managers can use third-party management tools to protect configuration data, such as encryption keys, in secure ME memory. ● Virus may corrupt or steal local data.	● There is no local data to corrupt. ● Users cannot work if the server is unavailable.
2. Unauthorized access to information (20.23 percent)		
Non-virus threats include the following: • Software/internal (e.g., browsing sensitive server files)	The items below address client vulnerabilities. Servers are also vulnerable. On a server-by-server basis, both client types are equally vulnerable to unauthorized server access, because IT controls that access. Because each server represents a potential entry point, solutions requiring more servers, such as thin clients, provide more server targets for intruders.	
• Software/external (e.g., hacking)	● Intel® vPro™ processor technology-enabled third-party management tools using Agent Presence and System Defense can help IT managers detect threats and keep security software running.	● Client devices are extremely difficult to hack.
• Physical (e.g., copying data to removable media)	● Intel® vPro™ processor technology-enabled third-party management tools that use Secure Memory, such as Cisco Security Agent, enable IT managers to configure clients to boot successfully only from authorized media. Doing so prevents intruders from booting from a USB drive or CD. ● Active Directory lets IT managers disable write access on USB ports on a network-wide basis using Group Policy.	● Client device may not offer connections to removable media.

	Intel® vPro™ processor technology and Intel® Centrino™ Pro processor technology	Server-based computing with thin clients
Vulnerability to software intrusions	● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools to run security software virtualized in "security appliances." ● Intel® vPro™ processor technology-enabled third-party management tools that use hardware and software filters can quickly detect suspicious behavior. ● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools to protect configuration data, such as encryption keys, in secure ME memory. ● IT managers can use encryption to help secure data. ● Successful hacks can be difficult to detect.	● Client contains almost nothing a hacker can attack. ● IT managers must assume greater responsibility and take greater precautions to ensure server security.
Vulnerability to physical intrusions	● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools and Intel® AMT to lock a stolen client and send a warning. ● IT managers can use encryption to help secure data. ● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools to protect configuration data, such as encryption keys, in secure ME memory. ● Notebooks are attractive to thieves because hardware has value outside of network.	● Inexpensive and limited-use hardware has minimal attraction to thieves.
3. Notebook or mobile hardware theft (12.65 percent)	● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools and Intel® AMT to lock a stolen system and send a warning. ● Intel® vPro™ processor technology includes chip-level TPM 1.2 support, which enables more secure hard disk encryption software, such as Microsoft * BitLocker. ● IT managers can use Intel® vPro™ processor technology-enabled third-party management tools to protect configuration data, such as encryption keys, in secure ME memory. ● Notebooks are attractive to thieves because hardware has value outside of network.	Mobile devices are not yet a significant presence.
4. Theft of proprietary information (11.49 percent)	Issues are identical to those for Category 2, Unauthorized access to information.	
5. Denial of service (DoS) (5.57 percent)	Both computing models are, for the most part, similarly vulnerable to DoS attacks against the server. Because each server creates a point of potential vulnerability, models using more servers, such as server-based computing, can be more vulnerable. Also, should a DoS attack cause a server to go down, because thin clients are unable to work locally, all clients using that server also go down.	
6–8. Financial fraud (4.87 percent), **Insider abuse of network access/e-mail** (3.52 percent), and **Telecom fraud** (2.40 percent)	Categories 6 to 8 involve individuals misleading others or misusing their legitimate resources and privileges. Because no computing model can distinguish between misuse and legitimate use, both models are equally equipped—or ill equipped—to prevent these losses. For this reason, we do not compare the computing models on these sources of loss.	

Appendix A: The top eight threat types

The 2006 CSI/FBI Computer Crime and Security survey does not define its risk categories. In this appendix, we provide our definition of each category. Because the survey based categories on financial losses, categories overlap when we view them from the perspective of technical security.

1. **Virus contamination.** Virus contamination accounts for 29.89 percent all of losses. Because the survey does not distinguish the different types of malware, we consider this category to comprise all types of malware, including viruses, worms, Trojans, adware, spyware, rootkits, loggers, etc.
2. **Unauthorized access to information.** Unauthorized access to information accounts for 20.23 percent of losses. We exclude proprietary information from this category, because that has its own category below. Common targets would be HR or financial data. Non-virus intrusions include:
    - Software/internal (e.g., browsing sensitive files on server)
    - Software/external (e.g., hacking)
    - Physical, such as copying to removable media
3. **Laptop or mobile hardware theft.** Laptop or mobile hardware theft accounts for 12.65 percent of losses. Although a mobile server-based computing client device may well be relatively uninteresting to thieves, these devices are still rare. (See http://www.principledtechnologies.com/clients/reports/Intel/ThinClientWP.pdf for a discussion of this.) The remaining client types are equally vulnerable to theft. Because the potential loss due to compromised data can be many times the cost of the hardware, this paper focuses on how each platform keeps data safe.
4. **Theft of proprietary information.** Theft of proprietary information accounts for 11.49 percent of losses. Common targets are the same as for unauthorized access to information:
    - Software/internal (e.g., browsing sensitive files on server)
    - Software/external (e.g., hacking)
    - Physical, such as copying to removable media
5. **Denial of service (DoS).** A denial of service attack is an attempt to make a computer resource unavailable to its intended users. The term most commonly refers to attacks against a server, such as flooding it with requests, which none of the client types can prevent or lessen. However, some people define denial of service more broadly to include malware, which affects client machines as well as servers.
6. **Financial fraud.** The definition of financial fraud we use is broader than its strict legal definition in many states. We use the definition from http://www.unmc.edu/ethics/words.html#F: "a deception practiced on another party to cheat them out of money." None of the client types are able to stop this type of fraud.
7. **Insider abuse of network access or e-mail.** Each organization's Internet use policy determines what constitutes abuse. Examples include using the corporate network for viewing pornography, shopping, visiting sports sites, and trading stocks. Examples of e-mail abuse include sending personal messages from a work account, harassing others inside or outside the organization, and impersonating another person.
8. **Telecom fraud.** Telecom fraud is typically less well defined than financial fraud. http://www.issa-sac.org/library/index.php?ID=7&i1=86 lists the following types of activities as types of telecom fraud: life-threatening calls, threats of violence, harassing calls, social engineering calls, PBX hacking, long-distance fraud, voicemail fraud, faxback fraud, wireless fraud, and pager fraud. None of the client types can do anything to prevent telecom fraud.

Note. Many common security threats—such as port scanning and denial of service incidents—attack the server and therefore fall outside the scope of this paper. However, attacks that infect the server or cause it to shut down will stop all work on thin clients, whereas both models that use rich clients have some ability to work locally if the server is unavailable.

Principled Technologies, Inc.
1007 Slater Road, Suite 250
Durham, NC 27703
www.principledtechnologies.com
info@principledtechnologies.com