Various Schemes to Speed up the PC during Virus Scan

Neha Bishnoi *(Author)*
Department of Computer Science
Manav Rachna International University
Faridabad, India
Neha.bishnoi@yahoo.com

Prof. S.S Tyagi *(Author)*
Department of Computer Science
Manav Rachna International University
Faridabad, India
shyamtyagi@hotmail.com

***Abstract*— The current threat landscape is changing and we have seen a large volume of new viruses captured by security vendors each day. Customers always complain that anti-virus software slow down their computers by consuming much of PC memory and resources. Antivirus developers have to keep on inserting new virus signatures into their databases as variety of zero-day threats over the internet are becoming more popular. Due to this large database anti-virus soft ware slows down the PC. However, the increasing size of the signature file is not the only reason to drag computers to a crawl during the virus scan. Many antivirus products are available in the market claiming for the safest and more efficient antivirus. In this paper we will also focus on the other reasons which contribute in slowing down the computer system during virus scan. Distributed anti-virus scheme becomes a popular solution for this problem. In this paper we will discuss the distributed security infrastructure for deploying a light-weight and fast anti-virus product and will also elaborate the different schemes responsible for slowing down the computer systems and suggested solutions for the same. We have also discussed some problems related to Cloud Computing and some solutions to it in this paper.**

Keywords- *Anti-virus, viruses, PC speed, distributed anti- virus scheme.*

I. INTRODUCTION

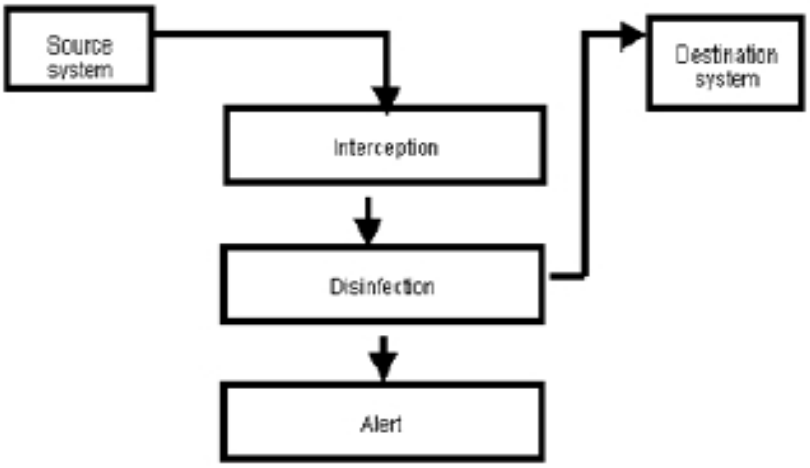
More than 100 new viruses are released and spread via the Internet every single day, making your antivirus software the most important program you have installed on your computer. Life in the antivirus software world is a constant game of 'catching up' because so many new viruses are released. It is absolutely crucial that you update your software as often as possible.

An anti-virus software program is a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware). To prevent viruses from entering a system there are basically just two options. The first of these is to place the computer in a protective 'bubble'. This in practice means isolating the machine; disconnecting it from the Internet or any other network, not using any floppy disks, CD-ROMs or any other removable disks. This way you can be sure that no virus will get into your computer. You can also be sure that no information will enter the computer, unless it is typed in through the keyboard. So you may have a fantastic computer, the perfect data processing.

The second option is to install an antivirus program. These are designed to give you the peace of mind that no malicious code can enter your PC. But how do they do it? How does the program let you install a game, but prevent a virus from copying itself to disk? Well, this is how it works.

An antivirus program is no more than a system for analyzing information and then, if it finds that something is infected, it disinfects it. The information is analyzed (or scanned) in different ways depending on where it comes from. An antivirus will operate differently when monitoring floppy disk operations than when monitoring e-mail traffic or movements over a LAN. The principal is the same but there are subtle differences.

The information is in the 'Source system' and must reach the 'Destination system'. The source system could be a



floppy disk and the destination system could be the hard disk of a computer, or the origin an ISP in which a message is stored and the destination, the Windows communication system in the client machine, Winsock.

The information interpretation system varies depending on whether it is implemented in operating systems, in applications or whether special mechanisms are needed. The interpretation mechanism must be specific to each operating system or component in which the antivirus is going to be implemented. For example, in Windows 9x, a virtual driver VxD is used, which continually monitors disk activity. In this way, every time the information on a disk or floppy disk is accessed, the antivirus will intercept the read and write calls to the disk, and scan the information to be read or saved. This operation is performed through a driver in kernel mode in Windows NT/2000/XP or an NLM which intercepts disk activity in Novell.

Once the information has been scanned, using either method, if a threat has been detected, two operations are performed:

1. The cleaned information is returned to the interpretation mechanism, which in turn will return it to the system so that it can continue towards its final destination. This means that if an e-mail message was being received, the message will be let through to the mailbox, or if a file way being copied, the copy process will be allowed to finish.

2. A warning is sent to the user interface. This user interface can vary greatly. In an antivirus for workstations, a message can be displayed on screen, but in server solutions the alert could be sent as an e-mail message, an internal network message, an entry in an activity report or as some kind of message to the antivirus management tool.

Scan Engine

Regardless of how the information to be scanned is obtained, the most important function of the antivirus now comes into play: the virus scan engine. This engine scans the information it has intercepted for viruses, and if viruses are detected, it disinfects them. The information can be scanned in two ways.

One method involves comparing the information received with a virus database (known as 'virus signatures'). If the information matches any of the virus signatures, the antivirus concludes that the file is infected by a virus.

The other way of finding out if the information being scanned is dangerous, without knowing if it actually contains a virus or not, is the method known as 'heuristic scanning'. This method involves analyzing how the information acts and comparing it with a list of dangerous activity patterns. For example, if a file that can format a hard disk is detected, the antivirus will warn the user. Although it may be a new formatting system that the user is installing on the computer rather than a virus; the action is dangerous. Once the antivirus has sounded the alarm, it is up to the user whether the danger should be eliminated or not. Both of these methods have their pros and cons. If only the virus signatures system is used, it is important to update it at least once a day. When you bear in mind that 15 new viruses are discovered everyday, an antivirus that is left for two or three days without being

updated is a serious danger.

The heuristic system has the drawback that it can warn you about items that you know are not viruses. If you have to work with a lot of items that may be considered dangerous, you could soon tire of the alerts. Programmers in particular may prefer to disable this option.

Permanent and on demand scans

When describing antivirus programs, it is important to clearly distinguish between the two types of protection on offer. The first is permanent scans, which are more complex and essential. These scans constantly monitor the operations performed on the computer to prevent any kind of intrusion.

The other type of protection available is on demand scans. These use the same scan engine as the permanent protection and check any parts of the system whenever the user wants. These are normally used under special circumstances. For example, a user may want to perform an on demand scan when using a new floppy disk or to check information stored on the computer that hasn't been used for a while.

II. WHY PC SLOWS DOWN?

The signature file can be considered as a malicious fingerprint database which is updated frequently to cover the latest threats. It works with the scan engine to detect threats. A big signature file will drag down computers tremendously.

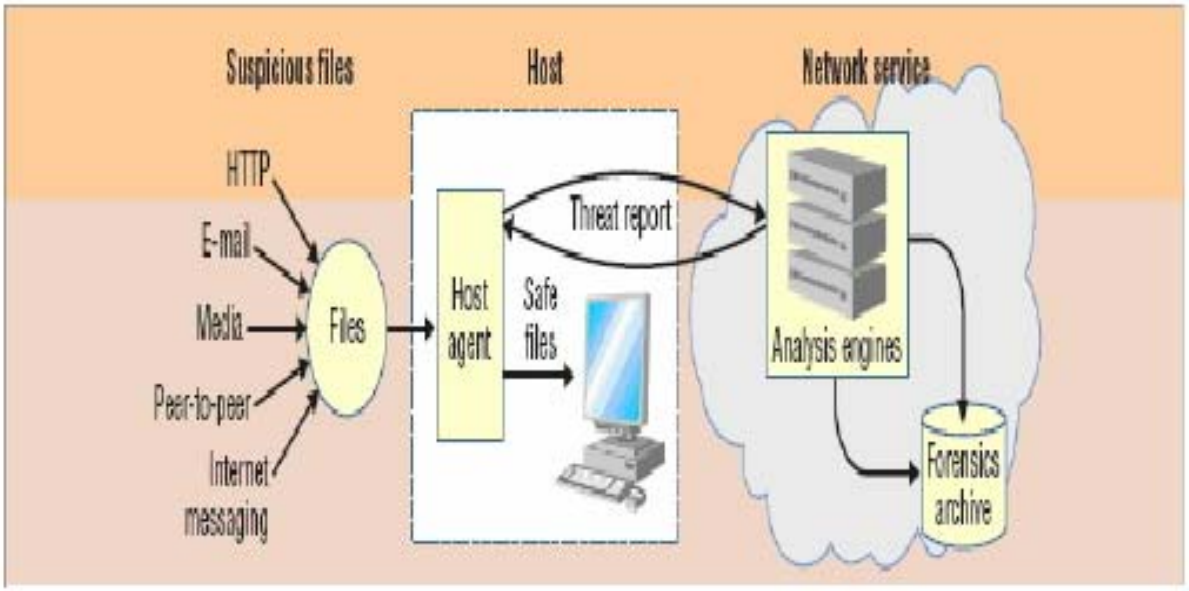
The PC spy (http://www.thepcspy.com/read/what_slows_windows_down/) had done an interesting testing to show how popular software applications slowed down Windows. Besides anti-virus softwares, Fonts, Yahoo's and AOL's chat programs, .NET, Visual Studio all slowed down computers quite a lot. This work even showed that 1000 Fonts had a bigger negative effect on the window load time than most AV products.

Three reasons for slowing down virus scan, that are actually not directly related to the size of the signature file.

(1) To evade detection, modern malwares are able to obscure their fingerprints and to make themselves undetected Portable Executable (PE) packers become the most favorite binary tools for malware authors to instigate code obfuscation. Thus, it is essential for AV scanners code obfuscation. Thus, it is essential for AV scanners to support the emulation functionality, which can safely analyze obfuscated malwares and then unpack their payloads. Yan et al. [13] discussed three approaches to cope with packers. However, malware emulation is very slow and expensive because it lets an executable file run within a virtual environment implemented by the software instead of the hardware.
(2) By hiding themselves deep into operating systems by using the rootkit technology, modern malwares can completely bypass personal firewalls and anti-virus scan- ners [14].
(3) The study in [15] showed temporal changes in the file size, file number, and storage capacity have increased over the past years. Accordingly, security products which scan data proportional to the number and size of files will take much
longer time.

III. ENHANCE SPEED WHILE AV SCAN

A countermeasure to speed up the virus scan is to move AV functionality from the user desktop into the cloud. It provides reliable protection service delivered through data centers worldwide which are built on virtualization technologies. It is a software distribution model in which security services are hosted by vendors and made available to customers over the Internet. This approach employs a cloud server pool which analyzes and correlates new attacks, and generates vaccinations online. The cloud infrastructure will sharply reduce computation burdens on the clients, and enhance security products in mitigating new malwares. Furthermore, customers only need to maintain a small and light- weight version of a virus signature file instead of the full copy Benefits include easy deployment, low costs of operation, and fast virus detection.



The agent is an on-access scanner deployed at the desktop. It places itself between the applications and the operating system. The agent automatically examines the local machine's memory and file system whenever these resources are accessed by an application. For any suspicious file, the agent generates the hash value or a specific signature of the file, and sends it to the remote cloud server for security verification. The low-latency anonymous communication network is used to forward these requests from the desktop to the remote cloud

IV. SECURITY CONCERNS

What are the "security" concerns that are preventing companies from taking advantage of the cloud? The Cloud Security Alliance's initial report [39] contains a different sort of taxonomy based on 15 different security domains and the processes that need to be followed in an overall cloud deployment. We categorize the security concerns as:
I Traditional security
II Availability
III Third-party data control

TRADITIONAL SECURITY

Concerns in this category include:
I. VM-level attacks. Potential vulnerabilities in the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architectures. Vulnerabilities have appeared in VMware, Xen, and Microsoft's Virtual PC and Virtual Server. Vendors such as Third Brigade mitigate potential VM-level vulnerabilities through monitoring and firewalls.
II. Cloud provider vulnerabilities. These could be platform- level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com. For instance, there have been a couple of recent Google Docs vulnerabilities and the Google response to one of them is here: There is nothing new in the nature of these vulnerabilities; only their setting is novel. In fact, IBM has repositioned its Rational AppScan tool, which scans for vulnerabilities in web services as a cloud security service.
III. Phishing cloud provider. Phishers and other social engineers have a new attack vector, as the Salesforce phishing incident shows[1].
IV. Expanded network attack surface. The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases. For instance, shows an example of how the cloud might attack the machine connecting to it.
V. Authentication and Authorization. The enterprise authentication and authorization framework does not naturally extend into the cloud. How does a company meld its existing framework to include cloud resources? Furthermore how does an enterprise merge cloud security data (if even available) with its own security metrics and policies?

VI. Data Loss or Leakage There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. unauthorized parties must be prevented from gaining access to sensitive data. Examples-Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; persistence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.
VII. Insecure Interfaces and APIs Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs.
VIII. Malicious Insiders. The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

Availability

I. Uptime. As with the Traditional Security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud user's own data centers. Besides just services and applications being down, this includes the concern that a third-party cloud would not scale well enough to handle certain applications.
II. Single point of failure. Cloud services are thought of as providing more availability, but perhaps not - there are more single points of failure and attack.
III. Assurance of computational integrity. Can an enterprise be assured that a cloud provider is faithfully running a hosted application and giving valid results.

Third-party data control

I. Due diligence. If served a subpoena or other legal action, can a cloud user compel the cloud provider to respond in the required time-frame? A related question is the provability of deletion, relevant to an enterprise's retention policy: How can a cloud user be guaranteed that data has been deleted by the
cloud provider?
II. Auditability. Audit difficulty is another side effect of the lack of control in the cloud. Is there sufficient transparency in the operations of the cloud provider for auditing purposes? Currently, this transparency is provided by documentation and manual audits. A related concern is proper governance of cloud-related activity. It's easy, perhaps too easy, to start using a cloud service. Certain regulations require data and operations to remain in certain geographic locations. Cloud providers are beginning to respond with geo-targeted offerings. Consumers at least seem to have decided that, in this case, the dangers of placing their data in the cloud were outweighed by the value they received.

III. Data Lock-in. How does a cloud user avoid lock-in to a particular cloud-computing vendor? The data might itself be locked in a proprietary format, and there are also issues with training and processes. There is also the problem of the cloud user having no control over frequent changes in cloud-based services. Coghead [2] is one example of a cloud platform whose shutdown left customers scrambling to re-write their applications to run on a different platform. Of course, one answer to lock-in is standardization, for instance GoGrid API [3].

IV. Transitive nature. Another possible concern is that the contracted cloud provider might itself use subcontractors, over whom the cloud user has even less control, and who also must be trusted. One example is the online storage service called The Linkup, which in turn used an online storage company called Nirvanix. The Linkup shutdown after losing sizeable amounts of customer data, which some say was the fault of Nirvanix [5]. Another example is Carbonite [4], who is suing its hardware providers for faulty equipment causing loss of customer data.

V. SOLUTION TO SECURITY ISSUES

Information-centric security

In order for enterprises to extend control to data in the cloud, we propose shifting from protecting data from the outside (system and applications which use the data) to protecting data from within. We call this approach of data and information protecting itself information-centric(note that [7], [8] use this terminology differently). This self-protection requires intelligence be put in the data itself. Data needs to be self-describing and defending, regardless of its environment Data needs to be encrypted and packaged with a usage policy When accessed, data should consult its policy and attempt to re-create a secure environment using virtualization and reveal itself only if the environment is verified as trustworthy (using Trusted Computing). Information-centric security is a natural extension of the trend toward finer, stronger, and more usable data protection.

High-Assurance Remote Server Verification

Lack of transparency is discouraging businesses from moving their data to the cloud. Data owners wish to audit how their data is being handled at the cloud, and in particular, ensure that their data is not being abused or leaked. A promising approach to address this problem is based on Trusted Computing. Imagine a trusted monitor installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide "proofs of compliance" to the data owner, stating that certain access policies have not been violated. To ensure integrity of the monitor, Trusted Computing also allows secure bootstrapping of this monitor to run beside (and securely isolated from) the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a "proof of compliance", the code of the monitor is signed, as well as a "statement of compliance" produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies.

Privacy-Enhanced Softwares

A different approach to retaining control of data is to require the encryption of all cloud data. The problem is that encryption limits data use. In particular searching and indexing the data becomes problematic. For example, if data is stored in clear-text, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. Cryptographers have recently invented versatile encryption schemes that allow operation and computation on the cipher text. For example, searchable encryption (also referred to as predicate encryption; see [9], [10]) allows the data owner to compute a capability from his secret key. A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query, without learning any additional information.
Apart from ensuring privacy, applied cryptography may also offer tools to address other security problems related to cloud computing. For example, in proofs of retrievability the storage server can show a compact proof that it is correctly storing all of the client's data.

VI. CONCLUSIONS

Our work is motivated by the need of explanation why AV softwares drag down users' computers. In this paper we have showed that the large signature file is not the only reason for the slowdown. Cloud computing is the most popular notion in IT today. They go on to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing". While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud. Our vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security. Among these are tools to control and understand privacy leaks, perform authentication, and guarantee availability in the face of cloud denial-of-service attacks

REFERENCES

[1] http://www.ebizq.net/blogs/security_insider/2007/11/implicati ons_of_salesforce_phi.php
[2] Cloud Bursts as Coghead Calls It Quits. http://blogs.zdnet.com/collaboration/?p=349
[3] GoGrid API. http://www.gogrid.com/company/press- release
[4] Latest cloud storage hiccups prompts data security questions http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM
[5] Loss of customer data spurs closure of online storage service 'TheLinkup'.http://www.networkworld.com/news/2008/08110 8- linkup-failure.html?page=1.
[6] AOL apologizes for release of user search data http://news.cnet.com/2100-1030_3-6102793.html.
[7] EMC,Information-Centric Security.http://www.idc.pt/resources/PPTs/2007/IT&Internet_ Security/12.EMC.pdf.
[8] ESG White Paper, The Information-Centric Security Architecture. http://japan.emc.com/collateral/analyst- reports/emc-white-paper-v4-4-21-2006.pdf.
[9] Song, D., Wagner, D., and Perrig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in Security and Privacy. 2000
[10] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano G. Public Key Encryption with Keyword Search. In EUROCRYPT. 2004.
[11] Third Brigade. http://www.thirdbrigade.com
[12] Why Google Apps is not being adopted http://money.cnn.com/2008/08/19/technology/google_apps.fo rtune/index.htm
[13] W. Yan, Z. Zhang, and N. Ansari "Revealing packed malware," IEEE Security and Privacy, vol. 6, no. 5, pp. 65-69, Sep/Oct, 2008
[14] C. Kruegel, W. Robertson, and G. Vigna, "Detecting Kernel-Level Rootk- its Through Binary Analysis", Proceedings of 20th Annual Computer Security Applications Conference , pp. 91-100. Tuscon, AZ, December 2004.
[15] N. Agrawal, W. Bolosky, J. Douceur, and J. Lorch, "A five-year study of file-system metadata," Proceedings of the 5th USENIX conference on File and Storage Technologies , p.3-3, San Jose, CA, February 2007 authentication,

AUTHORS PROFILE

Neha Bishnoi received B.Tech degree in Information Technology from Maharshi Dayanand University in 2009 and is pursuing M.Tech. in Computer Science and Engineering. Her areas of interest are Security issues of computer system and speed of the computer system.

Dr. S. S. Tyagi received B.Tech in Computer Science and Engineering from Nagpur University and M.E from BITS, Pilani and Ph.D in Computer Science from Kurukshetra University, Kurukshetra. Presently, he is working as Professor in Computer Science and Engineering department in Manav Rachna International University, Faridabad. His areas of interests are Wireless Security, Mobile Ad hoc Networks and Wireless Mesh Networks.