Global Information Assurance Certification Paper

Communications - Let's keep it clean...
Ricardo Costa
April, 1st 2001

Introduction

I remember my first contact with a personal computer in 1986 (I guess): a IBM-PC XT 4.77Mhz with 640Kb RAM, no HD, two 5 1/4" Floppy Drivers (360Kb), CGA (green), DOS and GWBasic. I remember, also, people complaining about viruses. I still remember they saying: "You know, a friend of mine gave me this disk with a cool application but when I read it, somehow, my screen began to show a little "ball" bouncing around the screen and erasing my documents.". By that time, I found that computers are not so free of failures as people used to say.

Still today, we need to think about these things. With the Internet, everybody is connected, information and programs of any kind from anywhere in the world. Every single home page you click, every single e-mail you read, can bring problems. Sometimes you can conclude that it is out of control. Under certain point of view it is, but we can avoid most of these threats by ensuring that all the data we accept is "clean". But how do we do that? The answers is "clean pipes". Clean Pipes is about ensure that your communication pipeline is "cleansed", even by working only with trusted sources or by applying some filters to check if this data was tampered or if it brings some malicious code as a trojan horse or virus.

Effectiveness of a Clean Pipe Solution

There are two primary types of cleansing that can be implemented together (highly recommended):

- Cleansing of Malicious Code (Virus, Trojan Horses, Worms, etc)
- Content Filtering (Filter Web and/or E-Mail content to avoid innappropiate language, suspicious code and sexual content)

Implement "clean pipes" solutions successfuly depends on the softwares you choose to protect your data and policies. When corporations think about softwares to secure their data, they analyze these points:

- *Scalability*: the software needs to support new hardware configurations as more memory and more processors to support bigger demands
- *QoS - Quality of Service*: the software needs to support intense traffic and find ways to handle these spikes
- *Availabilty and Reliability*: the software needs to keep alive even under heavy traffic or unappropriate conditions
- *Serviceability*: the software needs to support different protocols and services as the technology grows (HTTP, FTP, SMTP, IPSEC, etc)

- *Performance*: the software needs to secure the communications pipeline but cannot degrade users or system performance
- *Manageability*: the software needs to provide ways to ne managed and inforce the security policies designed for a company or a end user
- *Usability*: The software needs to accomplish its complex missions but cannot be so complex to be configured and managed (ease of use)
- *Customization*: the software needs to be customizable to fit company and end user needs
- *Support*: the customers that implement clean pipes solutions need support available to help them if something goes wrong
- *Cost-Effective Integration*: a company may have a mix-and-match systems and the software must easily integrate in their infrastructure
- *API-Level Integration*: some softwares need to plug directly into a proprietary systems and the this integration can be at the source code level

Effective Cleansing (and prevention) of Malicious Code

With the Internet viruses, worms and trojan horses spread widely and really fast. When we talk about "clean pipes" we must plan how we will protect our communications pipeline from this kind of threat. Nobody wants to download a file that is actually a trojan horse that will open a backdoor so others can access your documents and/or control your computer to make it work on a DDoS (Distributed Denial of Service) attack.

Viruses can attack your computer on many ways: e-mail server, Internet download, infected CDs or Floppies, shared folders, etc. So, when we think about virus protection, we need to implement solutions that protects every "hole" in your network (Multi-Tier). Multi-Tier Virus Solutions is about protect your firewall and gateways, file/print servers, groupware servers and workstations.

We need to remind that these solutions need to have a good defininitions update policy. The definitions update, to be effective, needs to be automatically and silently distributed accross a network to avoid user intervention and/or misuse and to make administrators be sure that the network is virus protected. Also, we need to inforce virus protection policies as we do in security policies. Administrators need to have a central point of administration from where they can easily configure the product and check for auditing data (logs, histories, scheduled scans, etc.).

Another great point is about new (unknown) unknown viruses. Symantec, for example, uses a technology called BloodHound that analyzes all files by its behaviour to find out if one particular file is taking suspicious actions on the system and then, if positive, the file goes to a central secure location called Central Quarantine for further analysis. To know more about Symantec AntiVirus Enterprise Solution, point your web browser to www.symantec.com and check the product features as well antivirus technologies.

Effective Content Filtering

If you search the Internet for data about misuse of companies Internet infrastructure you will be amazed. Companies waste several thousand dollars in infrastructure (communication links, software, hardware, etc) to support the every day growing demand for on line performance. They are not wrong, I agree, but we all need to agree that these same channels are not used as we would like to be. Some institutions placed some studies and found that something about 85% of the accesses made to pornographic, stocks, chat and sports sites occur during business hours.

Content Filtering is more than make your employees work better: it is about security too. If you have your communication link used wrongly, you will be always vulnerable to unauthorized downloads (virus, hackering tools, etc) and, maybe worse, sexual or inappopriate content that can lead your company to a harassment suit.

Companies often think that if they have a Firewall or a Proxy Server, they are already protected. We know that is not true. A Firewall only gives the company ways to control WHAT type of service is allowed in the network. Proxy Servers give the company ways to control WHO can access this or that site. Content Filtering is about the QUALITY of information your users can access. With Content Filtering solutions, like Symantec I-Gear, the administrator can give access differently per user, per group of users, per hour of the day, per client (IP Address) and so on. With Symantec I-Gear you can also input words like a dictionary and then, when a user access a web site that your Proxy or Firewall doesn't know, the product "reads" the HTML content to find those words you classified as Denied. This way, you will have an effective content filtering policy because it adapts according to every day needs.

Content Filtering is not only for HTTP traffic: SMTP traffic is also an issue. If you try to study your company's SMTP traffic you will certainly be surprised about how many e-mails are sent and received with unauthorized content, sexual or inappropriate words, useless attachments like funny movies, jokes, images, etc. I saw many administrators complaining about their SMTP and Groupware servers: "It's so slow" - they say.

I cannot predict how your company's e-mail traffic is but certainly it can be filtered. E-Mail is a powerful tool day after day it is becoming more important to users than the old-fashioned phone. Like Symantec I-Gear, Symantec Mail Gear gives the administrators a chance against innapropriate e-mail content (sexually oriented content, suspicious files, useless attachments, spam, black mail, etc). With a Content Filtering solution, you will be able to increase employees productivity, avoid harassment suits, prevent inappropiate content and make your infrastructure faster because your bandwith is not filled with useless traffic. Along

with that, your network becomes more secure because users that don't visit suspicious web sites are less vulnerable to viruses and hacker attacks. To find more about Symantec I-Gear, Symantec Mail Gear and Content Filtering technologies, point your web browser to www.symantec.com.

Planning and Security Policies (Best Pratices)

Now that we already know what is Clean Pipe solutions and some technologies that we can use to implement it, we need to understand, in may opinion, the most important part: PLANNING and POLICIES.

When I was a developer I used to work 80% planning and studying and 20% implementing. Maybe it is not the best rate but for me it worked fine because in the planning phase I was able to understand the whole problem, build a roadmap/schedule, foresee any possible problem and create an emergency plan in case of unpredictable situations as they occur. For Clean Pipes solutions, you should think about these points:

- What your company has (infrastructure)?
- What is important for us and for the others?
- What will be the impact of this solution (security x convenience)?
- What products we will use?
- What is the budget for this project?
- What is the roadmap to implement it?
- What if something wrong happens (emergency response team / support)?

You can think several more questions that are also important in planning but my point is: the more you plan, more chances you have to have success, but don't forget the action, because you are planning something that needs to be executed (it costs money). When we talk about policies, we already had our planning sessions. Policies stands for HOW things will work, most of times it is divided in two different documents or target audiences: technical and general policies. Technically, you need to write a policy to guide your Emergency Response and Support Team about how it needs to be implemented, like:

- Who have access to what systems and how the users will be authenticated?
- How the informations will be shared?
- How to install, configure, update and manage the software/hardware solutions?
- How to audit the network and systems being accessed?

Again, there are several other issues to be wrote here in the technical policies. The other policy document is planned to general audience (non-technical employees). Like any other security policy, you need users' satisfaction and support. Without that, your plan is targeted to fail. A general policy document should have informations like:

- What is a security policy?
- Why is your company implementing it?
- How the users will be affected?
- What the users should know?
- How the users can help?
- Best Pratices
- Liability

You may be thinking how hard it can be to plan and build a security policy. I can say that it is really hard but not impossible. I am sure you have heard about BS7799. BS7799 (British Standard 7799) was first published in 1995 by the British Standards Institute (BSI) and it is a set of guides to help you build an effective Internet security plan. BS7799 is now under International Standards Organization (ISO) consideration as ISO17799. If it is approved by its member, we will see major companies implementing its policies. BS7799 is divided into three major sections:

1. Standard Code of Pratice (or Best Pratices)
   - 10 major management areas, 127 security controls and 500 sub-controls to assist companies in protecting their assets
2. Implementing an Information Security Management System
   - Helps IT to prioritize network assets and organize those assets into a security plan that has four phases:
     . Risk Assessment
     . Risk Management
     . Safeguards
     . Statement of Applicability
3. Certification Process
   - Through a security audit, by a BSI-accredited thirdy-party consultant/auditor, the certification is completed

Future

In this document we discussed what is a clean pipe solutions, technologies, products, planning, policies, etc. I would like to remind you that it is not a buzzword or vaporware: it is a real need for every company that relies on the Internet to have their business (or part of it) running. Today most of us use a standard computer as their access device. The more you connect, less secure you are. The more technologies you create, more vulnerabilities come along. New threats are created every day, like viruses. New technologies are created to make our life easier but it opens new vulnerabilities for our operating systems, on computers, PDAs, oil companies, phone companies, etc. Network security is more important than simply have a firewall. Sometimes I can still catch myself missing those old times when I was working with my IBM-PC XT: it was really boring with we compare to today, but really, really secure. What we can do about it? Is the progress, right? So let's clean up these "pipes".

References

Symantec Corporation - "The Rise of the Network Trojan" - Dec 2000 - Eric Chien
http://enterprisesecurity.symantec.com/article.cfm?articleid=535&PID=3503647

Symantec Corporation - "Up to Standard: BS7799 and Your Enterprise" -Oct 2000
http://enterprisesecurity.symantec.com/article.cfm?articleid=356&PID=3503647

Symantec Corporation - "Understanding Clean Pipes Solutions" - Aug 2000 - Stephen Trilling
http://enterprisesecurity.symantec.com/article.cfm?articleid=192&PID=3503647

Symantec Corporation - "Worms and your Network" - Aug 2000 - Stephen Trilling
http://enterprisesecurity.symantec.com/article.cfm?articleid=245&PID=3503647

Symantec Corporation - "The Future of Content Security" - Mar 2000
http://enterprisesecurity.symantec.com/article.cfm?articleid=39&PID=3503647