Access Control for Applications

GIAC Security Essentials Certification Practical (Version 1.2f)

By

Bruce Thibault

On

January 31, 2002

Table of Contents

1 Introduction

Access control for applications is increasingly becoming a concern to the information security community. "Weak access controls for sensitive data and systems enable an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage.[1]" Access to protected data can cause the integrity of the data to be compromised and cause millions of dollars of harm. Unauthorized access by applications is especially serious in a networked environment. Trojan horses, backdoors, and spyware, can create potential points of vulnerabilities that can go virtually unnoticed by PC users and system administrators. Despite the threat, there are ways that personal pc users and network administrators to protect themselves. This paper will describe how access controls work, why they are needed, then it will discuss the threat associated by malicious applications followed by a discussion on software that PC users and administrators can use to protect themselves.

2 What are Access Controls?

According to the National Institute of Standards and Technology (NIST) Special Publication 800-18 "Guide for Developing Security Plans for Information Technology Systems" Access controls are defined as the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted."[2] Access controls are important in a computing environment because it helps enforce the principle of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Access controls ensure that people can only use the functions needed to perform their jobs, and functions that are critical (those needed for operation) are only performed by those who are authorized, trained, and capable of performing them.

Access control for applications works under the same principle as access controls for users. Applications are only granted access to the files and folders that are needed to run the application. Malicious applications that intend to write to a system file or applications that make use of services not needed introduce vulnerabilities to the system that can cause irreparable harm. These applications running unchecked on a computer creates vulnerabilities that a hacker could exploit.

[1] According to recent congressional testimony on November 9, 2001 by the U.S. Director of Information Security, Robert F. Dacey, to the U.S. House Government Reform Subcommittee on Government Efficiency

[2] NIST Special Publication 800-18, Section 8, Page 47

3 Why Are Access Controls Needed for Applications?

Access controls for applications are needed because there is an increasing threat to networks from applications that have unfettered access to either unauthorized files and/or services. Examples of applications that present these vulnerabilities are Trojan horse programs, programs that open ports (backdoors), And programs that use Spyware.

It is important to note that eliminating these threats is not the only obstacle in reducing the vulnerability of improper access controls for applications. Configuration management and policy development must also happen concurrently to correct any possible vulnerabilities. There needs to be standard set of rules (or Rules of Behavior) that govern what a user can and cannot do. Rules of behavior covers acceptable use of the Internet, what programs a user can download and what off the shelf software a user can install.

3.1 The Threats from Trojan Horse Programs

According to the third edition of Hacking Exposed: Network Security Secrets and Solutions "A Trojan horse is a program that purports to be a useful software tool, but it actually performs unintended (and often unauthorized) actions, or installs malicious or damaging software behind the scenes when launched."[3] Most of the time, the installation of these programs is often disguised so that the user will not notice their installation. Hackers will commonly package malicious code or programs along with legitimate programs in order to fool the user. The user will see that the executable that they performed actually performed an expected function. Typically they either arrive in an emailed game, joke, or executable. Once the Trojan horse has been installed on a computer, that system can be considered compromised. These Trojan horse programs can include programs that snatch username and passwords, open back doors on a computer, or introduce malicious code.

3.2 The Threat from Backdoors.

Backdoors and backdoor servers are usually the goal of a Trojan horse program. Backdoor programs and servers allow for remote access to a computer, usually without the users knowledge. Once a backdoor has been successfully opened on a computer there a variety of actions that a hacker can use to either gain control or steal information from a remote computer. These actions include:

[3] McClure Stuart, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. Osborne/McGraw Hill. 2001. 578.

- **Creating rogue user accounts** – Once a backdoor has been established a hacker can create additional user accounts with administrative access privileges and then use this new access to create even more accounts or use this privilege to alter system files.
- **Change startup files** – Depending on the operating system a hacker can introduce changes into the start up file that can cause malicious code or traps to open every time a user restarts his/her computer.
- **Install other backdoors** – Once a hacker has administrative control over a computer he can install other programs in harder to find places, so if one backdoor is found the others will still probably be there, thus the hacker insures that he will always have access to that particular computer.
- **Perform port redirection** – In order to bypass firewalls that have been installed on a system hackers will redirect packets that they want to send through common ports so that the user will not likely notice this activity.
- **Steal confidential or critical corporate information** – It goes without saying that if a hacker can create new accounts or install new programs, then a hacker can steal file or passwords on a compromised computer.

3.3 The Threats from Spyware

According to the Steve Gibson of Gibson Research Coporation, Spyware is “Any Software which employs a user's Internet connection in the background (the so-called "back channel") without their knowledge or explicit permission.” While the may seem harmless, it has the potential to be very dangerous. Spyware usually takes advantage of the fact that you usually “opt-in” installing spyware while installing a legitimate program. Companies hide this fact in the small print of user agreements and then use these back channels to obtain valuable data. While most of these programs are used to track user activity and track marketing data, the technology can be used for malicious purposes. Due to the constant tracking of user activity, Spyware can cause system and browser instability. Advertising Trojans make backdoor connections to applications running the background a computer that consumes bandwidth (and system resources) and may compromise the security of any classified or sensitive data. According to Ceex.org “The latest versions of these "ad-viruses" operate in full stealth and are nearly impossible to detect without advanced knowledge of the system environment. These include theTimeSink/Conducent TSADBOT and the Aureate advertising”[4]. There also examples of spyware applications that have been known to imitate system processes so that it cannot be terminated and does not appear on Windows' End Task dialogue. Spyware applications usually have automatic update and installation components that can operate without user control and it has been shown that it is “simple for a malicious user to hijack this capability to upload and run any program on a user's system.”[5]

[4] The Problem with Spyware and Advertising Supported Software: http://cexx.org/problem.htm
[5] http://cexx.org/problem.htm

4 Access Control For Applications – What Can be Done

As discussed previously, the threat that unfettered access by applications has to PC users and corporate networks are real. From Trojan horses, backdoors, and spyware there is plenty of opportunity for hacker or spies to penetrate and wreak havoc. A common solution that can be found to address this problem is addressed through the use of firewalls that block all outgoing connections without permission, however this is not a panacea. Firewalls are often mis-configured and many only block incoming connections. Once a system has been compromised a hacker can create additional ways to gain access. Additionally today's solution is often tomorrow's vulnerability. For example "Trojans are increasingly using outbound connections to pick up commands and avoid port blocking and intrusion connection, experts have said that firewalls may be highly susceptible these tricks"[6] Despite, the vulnerabilities, there are ways for home users and network administrators to protect themselves. The following discussion will detail programs that can help protect against the threat from applications using unfettered access to the Internet.

4.1 Access Control for Application Software for Home Users

Home PC users are particularly vulnerable to applications that contain Trojan horses and backdoor programs. This is true because of lack of expertise, a lack of knowledge about hacker techniques and a belief that PC users are not vulnerable to any threat. In the past the use of personal firewalls fell into the realm of "computer geeks" and/or "paranoid people" but are now becoming a standard feature found on computers that access the internet. There are several computer programs that are available to the PC user that are either free or can be obtained at a low cost. The following is a small sample of programs that are available and the services that they offer:

Zonelabs (ZoneAlarm and ZoneAlarm Pro) – Zonelabs offers a free firewall for home PC users that not only blocks incoming connections but also stops outbound connections without permission. Zonealarm screens outgoing communications and "whenever an application tries to connect to the Internet, Zonealarm Pro (and Zonealarm) intercepts its communications and forwards them to the Zone Labs, TrueVector engine. This engine, in turn, authenticates the application, protocol, and content. If the application had been previously approved to send messages, Truevector engine forwards the communication to the TCP/IP stack. Simultaneously, the engine notifies the firewall to let the connection pass. Only then will the Zonealarm Pro allow the application to communicate over the Internet."[7] Zonealarms is an excellent option to home PC users because they offer a fully functional free version. The pay version

[6] Middleton, James. Trojans Make Firewalls Futile. Vnunet.com. http://www.vnunet.com

[7] Guarding Your Remote Access VPN from Spyware and Targeted Attacks. Endpoint Security, From Zone Labs, Inc. Page 11

(ZoneAlarm Pro) offers additional options like Host Name lookup as well as other blocking of pop-up ads, etc. Although this service is free some users prefer to go with a larger name company like Symantec or McAfee.

Norton Personal Firewall – The Norton Personal Firewall (NPF) is another popular option that is available to home users. Like the Zonealarms firewall, NPF will also block all connections both incoming and outgoing. NPF also contains an "alert tracker that warns you about attacks and assures you that Internet traffic is actively being filtered"[8]. One drawback with the NPF is that it is more expensive than most of the other firewalls out on the market and you must pay to get continuing auto-updates on rules and service updates.

It is important to note that with these applications the firewall is not the only security factor. Most of these products are usually offered as a suite that either integrates with other programs, such as anti-virus software, or offers additional services for a price. For example, as we discussed before if a system is already compromised a clever hacker can find a way around any firewall. Zonelabs offers a program called pest control that will look for all known backdoors and close them before installing the firewall. In the case of NPF, it will integrate with other Norton Utilities so give the home user a comprehensive suite of programs.

4.2 Access Control Software for Enterprise Solutions

As with home users a user on a wide area network is just as vulnerable to Trojans, backdoors, and spyware. However there is additional level of concern because unauthorized access on a workstation can leave the whole network vulnerable and expose potentially classified or sensitive information. Because of the wide variety of workstations, a variety of severs in different locations, and an array of applications used; an enterprise can be extremely hard to secure. There is a growing concern among information security experts about access controls for applications. To help mitigate this threat, there are a variety of software solutions available that are suitable as enterprise solutions. As with the description of personal PC software that is available, this is only a sampling of software that is available and is not intended to be an all-inclusive list. Some software this is available on an enterprise basis is:

Okena's Stormwatch:- "Stormwatch 2.0 actually hooks into the OS kernel and provides application access control to system resources, such as reading and writing files, TCP/UDP port access as either client or server, and access to COM objects. It also restricts what applications, including which versions, are allowed to run the system. StormWatch uses a set of rules that define access policies, which are then deployed to host agents. When an application requests a

[8] Norton Personal Firewall. Key Features. http://www.symantec.com/sabu/nis/npf/features.html

resource from the OS, StormWatch matches the request to its policy and grants or denies the access accordingly."[9]

IBM's Tivoli – Tivoli is an offering that offers a smorgasbord of programs that an enterprise can use. Of particular is the Tivoli Policy manager in which the "Policy Director for MQSeries is also designed to provide access control services for local applications attempting to access remote queues, on servers running on platforms that its interceptor does not run on today. For example, Policy Director for MQSeries can prevent an application running on Solaris or NT from getting, or putting, messages to a local queue that maps to a remote queue actually on a Mainframe or AS/400."[10]

Purenetworking's Appsense – "Total control over application access can only be realized by a completely reliable and effective interception mechanism. The AppSense Agent meets these requirements by residing partly in the Windows NT Kernel. In doing so, AppSense can reliably intercept each and every request to execute an application, regardless of the source of the initiating request. For instance, the AppSense Agent will intercept attempts to launch applications from the Windows Explorer, DOS consoles and VB macros. This is possible because AppSense is not a user level solution that has to rely on a tight desktop policy or on extreme measures such as replacing the Windows shell and disabling useful tools. Instead it provides a totally transparent solution, and has no reliance on other system policies to function effectively. It complements existing NT security policies, such as domain level security and NTFS, resulting in a strengthening of the overall NT security."[11]

In order to be truly secure there must be a standard rules of behavior that is enforced throughout the enterprise as well as a comprehensive configuration management program. Along with software solutions, there must be sound policies and hardware solutions that complement any automated tools.

5 Conclusions

The threat that applications can pose to the security of either a personal PC or an entire work is real, therefore to mitigate the risk a set of access controls are needed to restrict unfettered access by programs with malicious intent. It has been proven that Trojans, backdoors, and spyware can pose a threat and both system users and network administrators must respond to these threats in order to minimize potentially damaging consequences. By staying vigilant, educated,

[9] Fratto, Mike. Safe Haven for Networks with Okena Stormwatch. November 12, 2001. http://www.networkcomputing.com/1223/1223sp2.html
[10] Tivoli Policy Director for MQSeries. IBM. http://www.tivoli.com/products/index/secureway_policy_dir_mqs/
[11] Appsense: The leading Application Access Control Solution for Microsoft Windows NT4 and Windows 2000 desktop and Server Based Environments. Purenetworking. http://www.purenetworking.net/Products/Appsense/Appsense.htm

and aware of best practices of the newest threats and mitigations one can stay ahead of the power curve and beat back any potential damaging attack. Technology advances so fast is today's security environment that vigilance is almost the most important aspect in securing an enterprise. Keeping up with alerts and threats and matching them with user behavior can mitigate the risk.

Bibliography

- Appsense: The leading Application Access Control Solution for Microsoft Windows NT4 and Windows 2000 desktop and Server Based Environments. Purenetworking.
- Dacey, Robert F. Congressional testimony on November 9, 2001 by the U.S. Director of Information Security,. to the U.S. House Government Reform Subcommittee on Government Efficiency
- Fratto, Mike. Safe Haven for Networks with Okena Stormwatch. November 12, 2001. http://www.networkcomputing.com/1223/1223sp2.html
- Guarding Your Remote Access VPN from Spyware and Targeted Attacks. Endpoint Security, From Zone Labs, Inc.
- Middleton, James. Trojans Make Firewalls Futile. Vnunet.com. http://www.vnunet.com
- McClure Stuart, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. Osborne/McGraw Hill. 200
- Norton Personal Firewall. Key Features. http://www.symantec.com/sabu/nis/npf/features.html
- The Problem with Spyware and Advertising Supported Software: http://cexx.org/problem.htm
- Swanson, Marianne. National Institute of Standards and Technology Special Publication 800-18. December 1998.
- Tivoli Policy Director for MQSeries. IBM. http://www.tivoli.com/products/index/secureway_policy_dir_mqs/
- http://www.purenetworking.net/Products/Appsense/Appsense.htm