Global Information Assurance Certification Paper

Securing the Enterprise with a Stateless Desktop Architecture

John C. A. Bambenek

February 20, 2002

Abstract

Desktop security has always been a problem for information technology professionals. Universities and corporations alike have always had problems with desktops being used and abused. With most security breaches starting on the inside, a solution needs to be developed to address the following problems:

- How can administrators possibly keep desktops secure when the users always seem to find ways around the policy?
- How do you prevent users from loading unauthorized applications on their machines?
- How do you prevent users from creating unintentional security holes on their desktops?
- How can the security team keep desktop users from abusive behavior on their desktops if the users have physical access to them?
- How do you audit logs (or use them after an incident) on hundreds of desktops?
- How can an administrator roll out security updates on hundreds or thousands of machines?
- How can an administrator keep control on what users can and can't do on their machines?
- How can you make sure that the desktop machines have the latest security updates?
- How can universities keep track of who is using their public computer labs?

These security problems and more are addressed with the utilization of a Stateless Desktop Architecture. A Stateless Desktop prevents users from having access to anything that could be exploited. In reality, there is nothing to exploit on the user end. By separating the processing hardware from the user, and only giving them access to a monitor and keyboard, there is nothing left for a user to break. Using Sun Ray technology as an example, this paper will show how to put the control back in the hands of the administrator and prevent users from being able to cause security problems overtly and inadvertently.

This paper is meant to provide information on a new technology that could increase security greatly. This paper does

not address all the possible aspects introducing this technology could have on an enterprise, but deals with how physical access to desktops increases vulnerability of some of the top 20 vulnerabilities published by SANS and the FBI and how a stateless desktop architecture can help mitigate it.

Introduction

> *"People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything" - Kevin Mitnick.*

One of the more critical security weaknesses that the enterprise faces is the fact that users are given a great deal of trust. An external attacker trying to gain information or an insider to rip off the company can use this trust. A great deal of this comes from the fact that users are given desktops that are plugged into the network.

According to the 2001 Computer Crime and Security Survey, 60% of attacks originated from *within* the company for those that responded to the survey. 91% reported employee abuse of information resources, and 94% reported having problems with computer viruses. (http://www.gocsi.com/prelea_000321.htm).

Sometimes users experiment with what is out on the internet to see what things can do and inadvertently end up opening holes for attackers to use. Some users are out to simply use their PC as a tool to attack the company itself. The problem comes in that whoever has physical control of the machine, has control of the machine. Administrator passwords and controls can only work so far. Users can still consciously or unconsciously circumvent them. They just don't think with a security mindset.

Users need computing resources to do their work. However, that physical access to those resources adds a degree of risk into the enterprise, and assumes a level of trust with the user. Company's try their best to educate users and hire employees with integrity, but according to the 2001 Computer Crime and Security Survey there are still incidents.

Enterprises can literally have thousands of desktops deployed for their users. Every time a security update is released, all of those machines need to be updated. This becomes

especially difficult when different users have different software loads. It becomes hard to keep track of who needs what patches, or more importantly, that every machine is as secure as it could be.

The Problems

DEFAULT INSTALLATIONS OF OPERATING SYSTEMS

Default installations of operating systems in listed as the #1 of the Top 20 vulnerabilities. By extension, this also includes unpatched systems or not-recently patches systems. Every operating system has security fixes that come out at least every month, sometimes more. If a company doesn't patch its' machines in a timely manner, they are vulnerable to a security hole that anyone could find out about worldwide. Most desktop users don't bother with security updates, and often, the IT staff is too busy to deal with patching because they are solving user problems.

ACCOUNTS WITH WEAK OR NO PASSWORDS

On many systems, accounts exist with weak or no passwords allowing for access to the machine with great ease. Every desktop has its' own password file and list of users. Protecting every one of these machines against weak or no-passworded accounts is an extremely difficult task.

SYSTEMS WITH LARGE BLOCKS OF OPEN PORTS

For a system on the internet, an open port is another gateway into a machine. Machines that have many open ports have that many more paths into the machine to protect. In addition, machines with large blocks of open ports are often flags of insufficiently protected machines and are subject to future attacks.

NO OR INSUFFICIENT LOGGING

Often times, if logs were checked regularly, security breaches could have been prevented. Logs contain telltale clues of probing wannabe attackers. Logs are also the first place incident handlers go for clues after an attack. With thousands of machines on the network, regularly viewing those logs is impossible. More often than not, logging is just turned off or ignored.

UNICODE, ISAPI, IIS RDS, AND NULL SESSION EXPLOITS

These are the standard Windows exploits used to wreak havoc in the Microsoft world. Every few minutes it seems there is another UNICODE scan going past every webserver. These are common and well-known exploits with automatic tools to exploit them.

NETBIOS / OPEN WINDOWS SHARES

Many users have a need to share files between desktops in an enterprise. However, most users don't take the time to protect any file sharing they do. They trust the environment is safe. However, many internal hackers use this to get information. In addition, many automated viruses and worms use these shares to spread throughout a company.

STANDARD RPC, SENDMAIL, BIND, R COMMANDS, LPD, SADMIND/MOUNTD, AND SNMP VULNERABILITIES

These are the standard UNIX vulnerabilities. They've been known for years, and tools to exploit them have been around for years. In addition to normal exploits, SNMP by default uses common strings to get information. These strings are well known, and if an administrator doesn't change the string on each an every device that uses SNMP, then anyone that can reach the machine can get a wealth of information about it.

There are too many different vulnerabilities to mention here, but they can lead to denial of service, unintended information release, or outright compromise if patches aren't installed in a timely manner.

FULL USER CONTROL OF THE DESKTOP

While not on the Top 20 list, this vulnerability sums up all the above and more. When someone has physical access to the machine, security mechanisms are less effective. In addition, companies tend to not really invest the resources in securing desktops from malicious users.

This is especially a problem in environments where computing labs are used (i.e. Universities). Not only is physical access there, but a level of anonymity is present. Users can walk up, cause trouble, and walk away making it hard to track who did it,

not to mention prevent it from happening in the first place. Even if password protection is used, all it takes is looking over one person's shoulder as they type it in at the lab, and they've got the ability to cause trouble and protect their own identity.

The Solution

Stateless desktop technology can mitigate these risks. As an example of this technology, Sun Ray devices remove the physical access to the information resources, but still provide the tools to do one's job.

A Sun Ray device is simply an input-output device that is plugged into the network that connects it to a main server. It functions much the same way an old xterm does with one main difference. There is no logic or technology in the Sun Ray to exploit or abuse. The only memory in the device is for the display, there is no processor, no disk, and no operating system. For all intensive purposes, it functions as a video card that plugs in into the network instead of a PCI bus.

The Sun Ray server and devices share a private network that only deals with Sun Ray traffic. The Sun Ray server is the only multi-homed device and is not configured to route traffic from the Sun Ray network to the outside network. In addition, the network, while using TCP, only send graphical and I/O information back and forth. It can be snooped, but the current tools would not be able to make use of the information.

The device then initiates a connection to the server and starts a graphical session. This session can be Windows or UNIX if the architecture is present for it. It then does all the processing and functioning at the server. Many users can be logged in, with unique desktops, performing unique tasks, all using centralized information resources that are physically protected. This technology can help mitigate the risks posed above in the Top 20 list.

DEFAULT INSTALLATIONS OF OPERATING SYSTEMS

In the case of an environment that uses a Sun Ray server, the only server that needs to be patched or updated is the Sun Ray server (except those that aren't "user machines" like the company mail server, etc). Instead of thousands of desktops needing to be upgraded, only the Sun Ray server needs to be patched. This also greatly reduces the effort it takes in

patching.

ACCOUNTS WITH WEAK OR NO PASSWORDS

All the desktop information in a Sun Ray architecture is stored on the server. This means only one password file for the enterprise. One password file can be audited much easy than a thousand. Also, it makes it more convenient for users because they only have to remember one password, which makes it less necessary to write passwords down.

SYSTEMS WITH LARGE BLOCKS OF OPEN PORTS

One thousand machines are always more difficult to control than one machine. Sun Ray devices don't reside on the network, but a private one, not to mention they can't be configured to listen for TCP services. The Sun Ray server is all that needs to be protected and secured. With only 1 server to close up ports on, it makes it much easier to get it done.

NO OR INSUFFICIENT LOGGING

One of the ways to mitigate insufficient logging is by utilizing central logging. This allows for only one information source to be checked for problems. In a Sun Ray environment there is only one source to be checked for logging, the Sun Ray server itself. This allows for the ability of more robust logging of the users in an enterprise.

For instance, process level accounting can be installed to create a list of actions a user does when they are online. This makes it easy to catch troublemakers early, or have evidence after an attack.

UNICODE, ISAPI, IIS RDS, AND NULL SESSION EXPLOITS

While the Sun Ray architecture is built on Solaris, it can be used to access the Windows environment with extra software. Using Sun Rays to access windows like this allows for an xterm-like environment for Windows users with the look and feel of having their own desktop. Many Windows users were unaware that these vulnerabilities existed, or that they were even running IIS during the height of Code Red.

By having all desktop users accessing their workspaces via Sun Ray devices, the only system that had to be hardened, or

cleaned, would be the Windows server that they access. This, again, reduces the workload of security from thousands of systems to one or a handful as the case may be.

NETBIOS / OPEN WINDOWS SHARES

The Sun Ray environment erases the need for file sharing between machines. Because the users all access the Sun Ray server, they only need to create a directory that both users have permission to access. As far as the server is concerned, the data transfer is local. This eliminates that need for sharing altogether.

STANDARD RPC, SENDMAIL, BIND, R COMMANDS, LPD, SADMIND/MOUNTD, AND SNMP VULNERABILITIES

Standard UNIX exploits are easily eliminated by using standard UNIX patches. All of the above can be secured by patching (except SNMP) and because the Sun Ray architecture reduces the number of machines to be secured, only one server needs these fixes. It makes it much easier to secure a network, as well as audit it for these vulnerabilities.

For the case of SNMP, the strings only need to be modified on the Sun Ray server because the Sun Ray devices don't even know what SNMP is. It makes the configuration simple.

FULL USER CONTROL OF THE DESKTOP

This is where the benefit of the Sun Ray devices and stateless desktop architecture is clearly seen. Users don't have control of anything. Users have the permissions that the server grants them, and they can't simply slip in a boot disk and try to override the operating system. It takes the control out of the hands of the users and puts it into the hands of the administrators. Because only the Sun Ray server (or any server they'll access with the Sun Ray) needs to enforce least privilege, it becomes a whole lot easier to enforce. Again, enforcing a policy on one server is easier than on a thousand desktops.

In addition, the desktop network would be a private Sun Ray network which doesn't route. Even if users plugged in laptops, they wouldn't be able to beat on anything except the Sun Ray server which should be well secured. Unless it is a Sun Ray device, it can't get any access to the Sun Ray server without

attacking it directly (as no services should be listening on that interface) which adds that much stronger of a layer of protection for the enterprise. While not allowing desktops may or may not be feasible in a given environment, it does provide for an option to create an even tighter network by not even allowing for unauthorized devices to get access to network resources.

ADDITIONAL SECURITY BENEFITS

Sun Ray devices come with a smart card reader that can be used for authentication. This authentication, when paired with the standard username/password challenge, creates a system of strong authentication. It makes it even harder to access network resources with a stolen password. One has to steal the smart card and the password, at which point, the victim user would realize they can't access to network and report they lost their card. This benefit is especially crucial for environments using computing labs because it makes it much more difficult to have anonymous access with a stolen password.

Sun Ray devices also allow a level of control of what resources users can access. A user can only initiate a desktop session on a device that the Sun Ray server is configured to see (the device also have to have Xwindows enabled). Once your on the system, additional controls can be placed at the system level to control where users can go (for instance, not allowing access to telnet or ping, or prohibiting users from accessing a certain machine). This can help keep users from scanning the network and doing things that might not be desirable in the eyes of the security team.

Conclusion

Using stateless desktops allows for centralized command and control of the desktop world. If the administrator wants to remove access to AOL Instant Messenger, for instance, it only has to be done at one place, the Sun Ray server. Permissions are controlled on the Sun Ray server and all logging and activity takes place on the Sun Ray server. This makes accounting and auditing easier by reducing the number of information sources.

The only machine visible to the outside is the Sun Ray server, which reduces the number of machines which need to be secured on a network. Sun Ray devices (or stateless desktops) aren't able to listen or answer to any network services and don't need any security. This reduces the overall workload of auditing

and securing systems in an environment.

The easiest way to secure a network is by minimizing access to the hardware and enforcing least privilege. Stateless desktops bring the control in the center were auditing, logging, and control are all centralized and protected. The easiest way to protect the desktop environment is to replace it with an environment where physical control of the machine isn't possible, and stateless desktops provide that benefit.

References

Alred, Douglas. "Awareness, A Never Ending Struggle". July, 2001. http://rr.sans.org/aware/struggle.php

Computer Security Institute. "2001 Computer Crime and Security Survey". http://www.gocsi.com/prelea_000321.htm

Ludwig, Katherine. "Security Awareness: Preventing a Lack in Security Consciousness". May, 2001. http://rr.sans.org/aware/lack.php

SANS Institute. "Mistakes People Make that Lead to Security Breaches". October, 2001. http://www.sans.org/mistakes.htm

SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities". November, 2001. http://www.sans.org/top20.htm

Smith, Kenton. "Security Awareness : Help the Users Understand". October, 2001. http://rr.sans.org/aware/help.php

Sun Microsystems. "Sun Ray Integrated Solutions". 2002. http://www.sun.com/products/sunray

Vosswinkel, Kerry. "Unique Security Challenges in Higher Education". September, 2001. http://rr.sans.org/casestudies/challenges.php

Wu Leng, Matthew. "Network Security Concepts and Essentials : A University Overview". September, 2001. http://rr.sans.org/casestudies/netsec_concepts.php

York, Wade R. "Weakening the Infrastructure from Within". April, 2001. http://rr.sans.org/start/weak_infra.php

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor