# Global Information Assurance Certification Paper

# Using Thin Client Architecture to Prevent Local Takeovers

**David L. Newman**
**GSEC Practical v1.4c**
**December 12, 2004**

## *Abstract*

This paper describes a solution to a common security issue: how to prevent a malicious user taking over a PC workstation if they have physical access and a means to boot the computer or inject code into it. The paper looks at the problem from an high level perspective and proposes that a thin client architecture would eliminate or reduce most of the exposures available in a traditional PC environment. It then describes some additional benefits of this type of architecture and looks at some issues and concerns that thin clients may create for implementors/administrators.

## *Introduction*

Most everyone has experienced it…

sitting peacefully, listening to a "hired gun security guru" work through their presentation, when all of a sudden, out of their pocket appears a floppy disk, cd-rom or a USB storage device with the "proclamation":

> ***"give me this media plus physical access to your computer and in fifteen*[1] minutes I will own your system."***

The genesis of this paper occurred during one such presentation. I found myself thinking... is this really true? Is there anything we can do to stop this? The security challenge this paper will attempt to answer is: if someone has media and physical access to your computer can they be prevented from breaking in?

To be honest, at the start of this project I did not have an answer, but my instinct told me that there must be a way to defend against this type of attack. I decided to do some research to see if I could come up with a viable defense for this type of security exposure.

This paper is a presentation of what I believe to be a viable solution for the security issue articulated above. To provide an overview of this issue the paper has been divided into the following sections:

> Section 1: Personal background and explains my motives and assumptions.
> Section 2: Proposed solution to the security issue.

1 This is a randomly chosen value, I have heard several variations. Please insert whatever number you consider valid.

Section 3: Additional benefits of my proposed solution.
Section 4: Review of issues and or concerns that need to be addressed.
Section 5: Conclusion.
Section 6: References and Recommended Readings

# Section 1 – Background and Assumptions

## Qualifications

My background is Unix/Linux Systems Administration (mostly in Sun Solaris), I am a certified Solaris System Administrator as well as a Redhat Certified Technician. I also manage several Windows networks for small business clients. I have also participated in several large scale technology implementations from both a technical and financial perspective and am currently active in several technology reviews with my current employer.

## Scope

The opinions and suggestions contained in this paper are derived from my personal experience, various conversations and interviews with other professionals and a generous amount of research and reading.

This paper contains no "code snippets" or how-to procedures. It is not meant to be a technical how-to but as "food for thought" and an overview of an architectural style that can reduce or eliminate the security issue stated earlier.

I will refrain from mentioning specific vendor solutions except where a vendor supplies a definite or unique solution for an architectural issue or a feature which I deem interesting and useful.

## Intended Audience

This paper is meant to be of interest to systems administrators, architects and security personnel who may not have had previous exposure to the proposed architecture or principals.

## Assumptions

***Assumption #1:***

> ***"The majority of today's users and administrators work in environments where their workstations have an attached keyboard, display and mouse."***

This assumption is based on the fact that Microsoft Corporation controls more than 90% of the desktop environment[23]. Accepting this assumption, we can then also assume the following two points to be true:

1. the workstation that is being targeted will have a floppy/cd-dvd/usb drive available.
2. the workstation that is being targeted will have a monitor and keyboard attached – or at least some form of input/output device.

***Assumption #2:***

We are dealing with a hypothetical vanilla environment. For reasons of space I will not try and think of exceptions to every point I will make in this paper. I understand that there will be many environments where what I propose is not feasible. However, I believe the architecture and ideas presented here are practical and worthy of consideration for most environments.

# Section 2 – My Solution

## Thin Client Architecture

The solution this paper proposes as the most appropriate for preventing local takeover of a PC or workstation is to use thin clients. This architecture eliminates the security problem that we are addressing and provides several extra security benefits.

Thin clients also have the added benefit of making very good business sense. It is beyond the scope of this paper to present a in-depth business case analysis but savings can usually be seen in the following areas:

1. Hardware Costs

A thin client will typically cost less than a PC and with no moving parts to wear out, a thin client has a life expectancy well in excess of a PC.

2. Labor Costs

Cost savings may be realized from efficiencies in labor. This is an area that needs to be studied closely by any organization that is considering migrating to thin clients.

3. Software Licensing Costs

In some examples software licensing costs can be reduced by moving away from Microsoft and other commercial vendor software. Sun Microsystem's Sun Ray product is an example of this, it runs on Linux and offers attractive software bundles and pricing.

---

2 Shankland, Stephen. "Red Hat aims desktop Linux at Microsoft." CNET News.com. May 04, 2004. URL: http://news.com.com/Red+Hat+aims+desktop+Linux+at+Microsoft/2100-7344_3-5205117.html

3 Gonsalves, Antone. "Windows Gains Market Share, Despite Linux Threat." TechWeb.com. October 08, 2003. URL: http://www.techweb.com/wire/26802826

It must be stressed that every situation is unique and what works for one organization may not work for all. The fact is that savings gains from conversion to thin clients are documented. For those interested in more details or studies see the recommended readings at the end of this paper.

## Defining the Problem

At first I looked at the challenge as a strict physical security issue. Could an intruder/malicious individual be prevented from taking over a workstation when they have physical access to the unit? However, as I researched it further I came to realize that this was not a physical access issue as much as it was a hardware and system access rights issue.

My original approach was that to solve the problem, physical access would have to be strictly monitored and controlled. This is not practical in most cases and not effective if the malicious person is an insider. To come up with an elegant solution I would have to look at the problem from a different angle. I then studied the fundamentals of the exposure, what exactly was needed to take over a workstation using external media? Basically, three elements are required:

1. physical access to the workstation
2. an input/output device to enter commands or observe the status of the workstation
3. physical medium with which to boot or inject control code

If any of these three pieces are removed, then the security risk is eliminated.

The first two items are nearly impossible to eliminate in a traditional workstation environment, as users need them to do their day-to-day tasks. The third item is not essential, so this is where I concentrated my efforts. The challenge became "how to prevent an intruder or malicious user from putting a floppy disk, cd-rom or a USB storage device into my PC?"

Once the problem was broken down in this manner it became relatively straightforward to develop a solution for a hypothetical "vanilla" environment[4]. A thin client architecture provides the most in-depth solution and allows the fewest possible attack possibilities.

At this point I should clarify exactly what is meant by thin clients. I am referring to hardware stations that have no internal hard drive and do no processing. All jobs are run on a central server or servers. Occasionally the terminology gets confused with Citrix style architectures where users still work from a PC at their desk. True thin client architecture provides users with a small hardware device that has no internal hard drives, no cd/dvd rom and (hopefully) no extra usb device ports other than those required for keyboard and mouse.

Obviously, it is possible to lock down a traditional PC using various techniques such as BIOS passwords and such, but in the end these techniques tend to be time consuming, hard to set up, difficult to enforce and open up a Pandora box of

4 I state this because in each unique environment there may be one to dozens of mitigating factors that will make the "hypothetical environment" solution unusable without modifications.

other issues. For example, BIOS passwords may prevent casual attackers, but the presence of BIOS passwords mean that they will have to be securely stored and a migration procedure will have to be developed for when administrators leave the team. Also, BIOS passwords will not prevent someone from quickly removing the hard disk drive and accessing the data later.

Thin clients remove these attack points and is therefore the best solution for our problem.

### Thin Clients May Require a Paradigm Shift

Considering that more than 90% of desktops are Microsoft Windows-based, we can expect that most of the administrators migrating to a thin client architecture from an existing traditional environment will be moving from a Microsoft/Intel based infrastructure.

For many of these administrators, moving to a true thin client architecture may be quite a large paradigm shift. Going from a workstation with hardware and software for each individual user to visualizing several larger machines servicing hundreds or thousands of users can introduce many new challenges.

My experience while participating in various security groups leads me to believe that most Microsoft-based administrators in large organizations are quite comfortable with the idea of “pushing” software updates or patches out to hundreds or thousands of clients regularly. The idea of thin clients is that you do your work on the server and let the clients connect – no “pushing” at all.

From the server side it can be a shock for someone not experienced in headless systems to walk up to a server and have no display, mouse or keyboard physically attached. I would expect the same level of initial disorientation for someone coming into a fully thin client architecture from a traditional PC based environment.

From a management perspective thin clients can also introduce challenges. Many cost models are based on per desktop licensing and support. Failed hard drives on PC's can mean hours to days of time for technical support and the end user. Thin clients can render large sections of traditional costing models irrelevant. One example would behaving no failed hard drives for local techs to replace.

## Section 3 – Additional Benefits of Thin Clients

In his section I will briefly address a few added benefits of the thin client architecture.

### Prevention of Take Away Theft

One of terminal server architectures greatest strengths – the ability to prevent, or at least reduce “take away” theft. By “take away” theft I refer to physically removing a computer from company premises or more commonly, the ability to save files to removable media and transport it from a secure area. Recent news

reports of missing data from nuclear sites show how the very presence of sensitive information on removable media can be an extreme security risk.[5][6]

### Introduction of Viruses, Trojans and Unauthorized Programs

In a thin client environment it is impossible for users to introduce viruses, trojans or unauthorized software into their work environment from their workstations because they do not have the usual introduction methods of floppy disk/cd-dvd/usb drives found in typical workstation environments. Note: This does not prevent downloading trojans and viruses from on line or network locations.

### Business Data May Not Be Backed Up

Many traditional PC based environments have important business critical data that is not backed up, either because it is not a drive/device that is part of a formal backup procedure or due to other user related causes (insufficient training, lack of software, no formal procedures, etc.)[7]

### Business Data May Be Stored in a Casual Manner

Businesses (or management in general) have very little control over how and where data is stored in a typical PC client environment. Users can (and do) store confidential, business critical unencrypted on local (or even in some cases shared) drives. The ability to police and ensure only authorized users are able to connect to shares is greatly enhanced when users have no possible way to share local disks over the network.[8]

### Disaster Recovery Planning

Physical terminal server units are worth a few hundred dollars each and consist of very few moving parts; this contributes to an expected long life with a replacement procedure of simply plugging the new unit in and powering it up. This simplicity greatly enhances DRP procedures. No desktop contains business critical data and the replacement procedure for clients is a simple as can be.

## Section 4 – Issues with Thin Clients

5 "US nuclear lab loses secret data." news.bbc.com. July 14, 2004. URL:http://news.bbc.co.uk/2/hi/americas/3898831.stm

6 "Missing Data." NewsHour with Jim Lehrer Transcript. June 13, 2000. URL: http://www.pbs.org/newshour/bb/fedagencies/jan-june00/data_6-13a.html

7 "The Business Continuity Conundrum." Gartner.com. 2004. URL: http://mediaproducts.gartner.com/gc/webletter/connected/vol2/issue4/index.html#indexa

8 Dewar, Helen. "GOP Aides Implicated In Memo Downloads." www.washingtonpost.com. March 05, 2004. URL: http://www.washingtonpost.com/ac2/wp-dyn/A31803-2004Mar4?language=printer

### *Systems Administration Adoption*

As mentioned earlier, using a thin client architecture may in some cases be a huge change in procedures and thinking for a system administration teams. Most thin client vendors are aware of this and have been actively developing documentation and procedures to ease the transition. See the recommended readings list for examples.

### User Adoption

Some users may rebel or complain if their "standard operating procedures" are changed. For instance, if a user is accustomed to transporting data using portable medium then they may find a terminal server/thin client architecture not very user friendly. Management should make all efforts to educate the users to the benefits of using this architecture and refine their expectations accordingly.

### Laptop Synchronization Issues

Timely laptop synchronization can be a major issue within some environments. Road warriors and executives tend to need access to data from various geographical locations at all times. Again vendors recognize this fact and are developing methods to deal with this disconnect. Note: The higher the laptop-to-employees ratio, the less attractive thin clients become. For instance, if 90% of the users have laptops, then thin clients are not a reasonable solution for an organization because the major benefits of thin clients will not be realized.

## Section 5 - Conclusion

### *Conclusion*

Researching and writing this paper has taught me that what the security guru was proclaiming was in fact in most cases:

1. true
2. not easy to defend

It was ***true*** because once you have media, combined with physical access; most any traditional workstation is yours for the taking. It was ***not easy to defend*** because unlike the movies most of the bad guys/gals were not easily identifiable and tended to be friends, work mates or trusted insiders.[9]

Researching and writing this paper has also taught me that what the security guru was saying is at the same time:

1. false
2. defensible

9 Littman, Jonathan. "Inside jobs: Is there a hacker in the next cubicle?." www.pcworld.com. August 13, 1998. URL: http://www.cnn.com/TECH/computing/9808/13/hacker.idg/

It is ***false*** because medium and physical access alone does not necessarily give someone the ability to take over your PC. It is ***defensible*** for simply the reason that it is not always true – one need only to figure out what the circumstances are when someone cannot take over a computer and mimic this as widely as possible and viola, a more secure setup. Thin client architecture is an architecture that will make this possible.

Much needs to be done before thin clients are recognized (or re-recognized) for their security strengths and values. Some technical obstacles must be overcome and some new ways of thinking will need to be introduced to the traditional desktop system administrators. However, the security benefits of this type of architecture are too great to ignore and for many organizations these benefits alone will make this a viable alternative in the future.

## Section 6 - References and Recommended Readings


1. Descriptions of City of Largo, Florida's success with thin client architecture.

Haber, Lynn. "City saves with Linux, thin clients." April 05,2002. www.zdnet.com. URL:http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2860180,00.html

Miller, Robin, "Largo loves Linux more than ever." December 09, 2002. URL:http://www.newsforge.com/business/02/12/04/2346215.shtml?tid=19

Orzech, Dan, "Across the Country, Local Governments Are Giving Linux a Hard Look." July 18, 2003. URL:http://www.cioupdate.com/trends/article.php/2237451

2. SANS paper describing SUN Sun Ray and other terminal services architectures.

Tanwongsval, Surachet. "Sun Ray Thin-Client and Smart Cards: An Old Concept With New Muscle." April 5, 2002. URL: http://www.sans.org/rr/whitepapers/terminal/320.php

3. SUN Microsystems documentation related to their SUN Ray thin client product.

http://www.sun.com/sunray/whitepapers.html?redirect=false&refurl=http://wwws.sun.com/software/sunray/index.html

4. Links to Wyse Technology, one of the major Windows/Intel thin client providers.

http://www.wyse.com/index.htm/overview/white_papers/index.htm
http://www.wyse.com/overview/success/index.htm

Last Updated: May 23rd, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |