# SANS Institute
## Information Security Reading Room

# Printer Insecurity: Is it Really an Issue?

Vernon Vail

# Printer Insecurity:
# Is it Really an Issue?

GSEC v 1.4b Option 1
Vernon T. Vail
May 28, 2003

## Introduction

Printers are an essential tool for today's business activities and therefore an essential component of today's network infrastructure. Aside from computers, printers are usually the most commonly used devices on a network. While much attention has been focused on computer security, there has generally been very little attention given to printer security. Questions, however, are beginning to be raised, especially as more and more institutions are employing network scanning tools to search for vulnerabilities, and they are usually finding them in places they didn't quite expect. There are now diverse opinions forming in the broad system and network infrastructure support world about this topic. It is becoming common to hear of contentious meetings and debates concerning real versus perceived threats and the potential reallocation of precious time and resources (equals money) to address printer insecurities.

So then, let's ask some questions. Are there really any significant printer vulnerabilities? Even if there are, should this really be a big concern? What are the attitudes of security professionals toward this issue? If there are problems, are manufacturers committed to fixing them? In short, are printer insecurities a relevant issue or not?

This document starts with a brief look at basic system and network security principles, continues with the revealing of some printer threats and vulnerabilities, and ends with a discussion about how to deal with the issue. To keep things brief and easily readable, many of the technical details of printer exploits are avoided. Even though information available on the topic of printer security is quite minimal, a little in-depth research and following up on any references listed here should find the pertinent details, if needed.

## Security Philosophy

Looking through popular security books and training course materials yields little, if any, specific information on printer security. These resources, however, outline an overall approach or philosophy to securing any device on a network. So before we discuss any specifics on printer security, let's take a brief look at the underlying principles of network security.

To begin with, there should be a clear understanding of the types of data that are being processed and therefore potentially being printed. It is now common to have sensitivity labels for data. What would be the most sensitive level of data that could be printed by anyone who can use the printer? What kind of damage could be done if that data were leaked?

Next is the real need to consider the possible *threats*. These could be anything that represents possible danger to your information. A threat can be either physical or electronic. The truth is that there are so many potential threats to data security that there can never really be complete protection from every possibility. There is a strong need, therefore, to identify what are the most likely and/or most damaging threats to each organization and prioritize them.

After looking at the threats, one should understand, as best as possible, any *vulnerabilities*. These are weaknesses in a system that could allow a threat to actually cause damage. Vulnerabilities can be mitigated or even eliminated, provided, of course that the system administrator knows about them.[1] A common problem is that many vulnerabilities lay undiscovered or undisclosed for a long time. Unfortunately, by the time they are widely revealed they have usually already been discovered and exploited by hackers.

What we then come to is a valuable formula for determining our *risk*: That is *Risk = Threat x Vulnerability*. Plainly stated, the risk of some form of security breach occurring is based on the possible threats and any vulnerabilities that may help bring those threats to fruition. If you have a high threat, but a low vulnerability to that threat, the resulting risk will be low. If you have a high vulnerability, but the threat is minor, once again the risk is low. If, however, there is a high threat and a high vulnerability, risk would also be high.[2]

*Security Policy* can also be an effective tool. Well documented and disseminated rules, procedures and consequences will help reduce security incidents in the first place, especially by an insider. Along the same line, thorough and organized *incident handling* will help test that security policy and guide future policy. Being able to detect and react to an incident in a timely fashion is extremely important.

A broad, helpful concept that ties all this together is known as *Defense in Depth*. Once there is a clear understanding of the types of data that is to be protected and what the risk factor is, there should then be some kind of strategy to protect that data. The Defense in Depth strategy says that there should be multiple protection layers in place so that if one fails, there are more layers behind it. (Example: Security policy states that no one can place

[1] Sans Security Essentials II: Network Security Overview, 2002, page 1-10
[2] Sans Security Essentials II: Network Security Overview, 2002, page 1-11

devices on the network without approval, but what if someone did? Are there mechanisms in place to find these devices? If someone were to use a misconfigured device against a network, are the other network resources adequately protected? Are there documented procedures about how to deal with this type of incident?)

Finally, it must be mentioned that effective security can only be achieved when there is *balance* between protection and usability. Consider whether protection measures make a device or service too inconvenient or even motivate users to attempt to circumvent the protection. A commonly reported example would be the password policy that is so stringent that users can't remember their passwords so they write them on sticky notes and tape them to the monitor. In this case, did the protection measure work as intended, or possibly create a bigger problem? Balance is also necessary when considering the workload of technicians who must often quickly or remotely service these devices.

**Know the Environment**

Now that we have reviewed some foundational principles, we can start to apply this understanding to the subject of printer security. As was previously mentioned, threats to an institution's infrastructure, both physical and cyber, should be listed and prioritized as to their criticality. This is something that can only effectively be done by someone who knows the environment, including the types of data being produced and protected.

Almost all organizations produce printed data that would be damaging to some degree if compromised or abused. Think of sensitive employee data revealed to other personnel. Think of personal financial data being used in identity theft crimes. The impact of poor printer security could be even more drastic when the printers are used for sensitive research data that would be highly destructive to a company if revealed to a competitor. Government agencies have vast amounts of secret data to keep safe from the public and from foreign governments.

To know the environment should also mean knowing several other important details such as the physical location of the printers as well as the functions and features of the various printer makes and models.

**Printer Threats & Vulnerabilities**

Threats such as fires, floods or earthquakes would usually not be as much of a concern to physical printer security as they would be to a data center with multiple servers. The next few paragraphs, however, should make it evident that easy physical access to a printer by an unauthorized person should be an item of concern.

Many modern network printers contain a hard drive to store print jobs. If the drive were to be removed, it could be connected to any PC and the data analyzed. Fortunately, some manufacturers use encryption schemes or wipe the data from disk after use. These methods, however, have been overcome by attackers before, so one should still consider what damage could possibly be done if data were to be successfully retrieved from the disk. Those responsible for security should know who services the printers, what is done with replaced components, and how older or non-repairable units are discarded.

Data can possibly be intercepted and sent to a third party using a number of methods. Firmware on some printers could be modified to add this ability or other special features such as a network sniffer. This could be done by either uploading modified firmware or by modifying and replacing a chip on the printer's circuit board. A network sniffer device can also be discreetly plugged into the printer's network port and can be programmed to either store or forward any packets that match a particular ruleset.

Consider how easy it would be to plug the printer's network cable into a laptop computer. This would enable a myriad of possibilities such as intercepting print jobs, searching for and attacking systems from behind the firewall, or even just browsing inappropriate web sites with less risk of getting caught.

A common printer configuration involves using a print server to allow for centralized print job management on several printers at once as well as employing mechanisms to control access. Because of these controls, many administrators mistakenly assume that access to the network printers has been limited. Users, however, can usually bypass the print server and access the printer directly. "There are some methods available to force people to use a print server (such as placing the printer behind a firewall and setting up a rule to allow the firewall to only pass packets to the printer from the print server"[3] Few organizations, however, are likely to do something like this for every printer on their network.

Transitioning to the electronic side reveals a whole host of potential problems. Printers today offer multiple protocols and services to allow for print jobs from a wide variety of environments. They also offer various methods of service and configuration. While all of this may allow for easier use, these mechanisms are often insecure and open the door to potential exploitation. Worse, these features can be difficult and sometimes even impossible to shut off, and they are usually turned on by default.

[3] Mattison, Dennis. "Network Printers and Other Peripherals – Vulnerabilities and Fixes." 27 April 2002 URL: http://freshmeat.net/articles/view/445 (15 April. 2003).

Telnet, FTP, HTTP, SNMP, and PJL are just some of the available options for using and servicing most modern printers. By using these and other services, an attacker can access printer settings to cause all sorts of havoc, as we will see. Incredibly, a large number of printers currently in service will allow unauthenticated access to their configuration information using many of these protocols. Others use authentication, but have well known default passwords that are rarely changed or in some cases cannot be changed.

SNMP (Simple Network Management Protocol) is a prime example. Network management applications can use SNMP to control and monitor some devices. It uses simple default passwords and is almost always turned on by default. Even if the password is changed, some printers store the administrative account password in an SNMP variable that can be read by any remote user that knows the address of the printer and the location of the variable.[4] The location of this variable has been published on the internet. Sniffed SNMP traffic can reveal a great deal about the structure of a network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks.[5] Of note: A newer and much safer version called SNMPv3 is now available on some of the newest printers. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over a network.[6]

Another example involves Telnet and is explained in the following excerpt from a Bugtraq listing:

> *HP JetDirect devices configured using the JetAdmin web interface do not set a password for telnet access when the administrator password is chosen. As a result, the telnet port will be left exposed to unrestricted remote access. Remote users with malicious intent will be able to access the device to cause a denial of service, or potentially monitor printer activity to gather information that may be used to compromise systems. Additionally, this problem is compounded by the fact that the admin password is reset when the device is rebooted. Workaround: Set the telnet password manually.* [7]

HTTP based management services are usually stripped-down versions of webserver software that are at revision levels that have widely documented security problems. Some printers are vulnerable to cross-site scripting exploits that try to fool a user into believing they are connecting to a printer's web server when they are actually talking to the attacker.[8]

---

[4] Ittersum, Shawn, "Vulnerability Note VU#377003." 6 Aug. 2002
URL: http://www.kb.cert.org/vuls/id/377003 (19 May. 2003)

[5] No author. "How To Eliminate The Ten Most Critical Internet Security Threats." 25 June. 2001
URL: http://www.sans.org/top20/top10.php (19 May. 2003)

[6] No author. "SNMPv3." 7 March. 2000
URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm

[7] Backman, Will. "HP JetDirect JetAdmin Password Vulnerability." 1 Aug. 2001
URL: http://www.securityfocus.com/bid/3132/discussion/ (19 May. 2003)

[8] Mattison, Dennis. "Network Printers and Other Peripherals – Vulnerabilities and Fixes." 27 April 2002
URL: http://freshmeat.net/articles/view/445 (15 April. 2003).

PJL (Printer Job Language) provides job status control by sending printer status information to an application. Its power allows job control that can't be accomplished with PCL (Printer Control Language) or Postscript. It can also control a printer's settings and its file system. It relies on a simple password that reportedly can be broken in less than 6 hours by a brute force attack. There are also hacker tools available which provide PJL communication to change settings and allow full file system access.

Some of the latest printer models run a Java Virtual Machine for embedded systems called "ChaiVM". There is a documented process available on the internet which shows how to force a custom ChaiJava application to be uploaded and run on a printer. There are already port scanner and password cracker applications freely available for this exploit.

Another potentially serious issue that is all too common, is the discovery of hidden "backdoors" that can allow very powerful configuration options. Unfortunately, some manufacturers have come to depend solely on the security principle known as "security through obscurity." They are betting that a secret password, hidden URL, or undocumented or difficult procedure will never be discovered or attempted. The problem is that if the backdoor or procedure is exposed (and it often is), the consequences may last for a long time since rarely are they quickly fixed by manufacturers and/or even known by administrators. A published example is the hidden web pages that were discovered on some Tektronix printers. These pages allow unauthenticated access and contain configuration options that are much more powerful than even a legitimate administrator of the printer can do. Worse, by going to the right URL you can actually read and modify the administrator password. [9]

Now that we know some of the access methods, what can be done with this power? One of the most obvious risks associated with unsecured printers is from a denial of service (DoS) attack. A DoS attack is usually very easy to perform and can be very frustrating for network administrators to overcome. Printers are especially vulnerable because fixes for known exploits are either not available or are slow to be delivered and/or implemented. While the vulnerabilities may be identical to those found in many other devices with an operating system, there is no control over the printer OS available to implement workarounds (other than firmware upgrade). Examples of this attack include HP printers that were affected by the Code Red Worm, printers that can suffer from a Telnet attack, others that are defeated by buffer overflows for FTP servers, and there are plenty more. The easiest DoS, of course, is to just overwhelm the printer with huge amounts of traffic so that it can't handle valid requests. An attacker could also simply change any of several printer settings (such as IP address) to cause a DoS.

[9] Mattison, Dennis. "Printer Vulnerabilities and Exploits"
URL: http://members.cox.net/ltlw0lf/printers.html (15 April. 2003)

The possibility of theft of sensitive information is probably the most worrisome to users and security professionals alike. Some previously mentioned methods include physically or electronically (PJL, FTP) accessing the printer's hard drive (some models may use a RAM disk instead of a hard drive) and using a network sniffer installed on a printer. Another possible point of manipulation is known as print job pooling. This is a setting on some printers that allow jobs to be forwarded to another location. The following excerpts from a post to the NTBugTraq list should help to underscore everything that has been mentioned so far in this document:

> *… obtaining the RAM contents of a HP JetDirect printer is actually quite easy to do…*
> *… the printer will TFTP the contents of RAM to the IP address that responded to it's BOOTP query. This implies that the printer must be configured to use BOOTP to obtain it's IP address. Surprise, this is also remotely configurable via SNMP…*
> *… a remote user can get a list of job descriptions sent to the printer. By continually monitoring the job descriptions, a remote person can use … to obtain copies of the 'juicy' documents as soon as they are printed…*
> *… it is quite trivial for someone to code something up that reconfigures the printer to use BOOTP, answer the BOOTP request, request the RAM contents, and then disable the BOOTP functionality on the printer. Parsing the RAM contents for print jobs is as easy as stripping out the PCL encoding, or by just splitting apart the print jobs, and sending them right back to the printer, as is. Additionally, seeing as SNMP is used during the HP JetDirect firmware upgrade process, theoretically one could code an exploit that uploads a trojaned firmware image…*[10]

Potentially even more dangerous is the ability by hackers to use some of the services running on a printer to assist in the gathering of information about a network. Some of them would really like to discover where the real data stores are located and how well they are protected. Surprisingly, a printer can make this much easier for them to do without being detected. We have already looked at the ChaiVM problem which could really assist hackers in their efforts. The following example is a brief explanation of what is called an FTP Bounce attack*:*

> *Many of the printers available on the market offer anonymous FTP servers for dropping print jobs into the printer. Unfortunately, many of these anonymous FTP servers allow passive mode FTP and the 'get' command, which makes them vulnerable to passive FTP forwarding. This allows the attacker to use the anonymous FTP server as a proxy server, forwarding all packets to the victim while hiding the attacker's true IP address. To the victim, the attacking machine appears to be the printer. … Since no logs are kept by the printer, bounced traffic is essentially anonymous and untrackable. Using the printer to hide the tracks, the attacker can scan the network, access sensitive information, and redirect network attacks without worrying about being discovered.*[11]

Looking again at the hard drive, if the printer supports PJL, an attacker may be able to download and upload files to and from a printer. This could be a relatively safe place to store hacking tools and stolen data since it is unlikely an investigator would think to or even know how to look there.

---

[10] Nash, Paul. "SNMP vulnerabilities." 14 Feb. 2002
URL: http://archives.neohapsis.com/archives/ntbugtraq/2002-q1/0106.html (30 April. 2003)

[11] Mattison, Dennis. "Network Printers and Other Peripherals – Vulnerabilities and Fixes." 27 April 2002
URL: http://freshmeat.net/articles/view/445 (15 April. 2003).

## What Should Be Done?

Before looking specifically at how to help mitigate some of these problems, let's once again go back and look at some of the foundational security principles. Have potential threats to the data been prioritized and the risk of attack been determined? Are there other basic measures already in place (firewall, good security policy) that may at least help prevent most attacks, even with vulnerabilities present? (Multiple layers – Defense in Depth). The reason this is being repeated again is that even after considering all that has been revealed so far in this document, (and just about anything else related to printer security), the fact is that printer security has received little attention not only from the good guys, but the bad guys as well.

Why is this true? It has been suggested that attackers may not know about the problems, or not know how to exploit them. Others think it could be because there have been so many other easier and potentially more fruitful methods available to them. One of the more likely reasons may be due to the increased attention that has been given to network security. Firewalls are being deployed just about everywhere. There is a relative inability to exploit most of these vulnerabilities by outside attackers. Most hackers are interested in internet exposed vulnerabilities, and most printers are not accessible to attack from the internet, from malicious email or from web-based malicious code, making them less attractive targets in most instances. Printers could, however, be an extremely attractive target to the insider. The relevance of this would depend upon how the organization weighs that threat. A re-read of the "threats and vulnerabilities" section of this document may prove beneficial in this light. It would still be prudent, however, to consider what may happen if a firewall was to be bypassed, such as a compromised VPN account (defense in depth). Something to keep in mind is that as the state of system and network security improves, attackers may have to resort to any method they can find to gain access.

The SANS Institute publishes and updates lists of the top 10 and top 20 vulnerabilities that are currently being exploited. Here is an excerpt from their web site:

> *The majority of the successful attacks on operating systems come from only a few software vulnerabilities. This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems. … Thousands of organizations use that list … to prioritize their efforts so they could close the most dangerous holes first.*[12]

[12] No author. "The Twenty Most Critical Internet Security Vulnerabilities." 3 March. 2003 URL: http://www.sans.org/top20/ (19 May. 2003)

Printer vulnerabilities have very seldom been on any kind of list such as this (SNMP may be the exception on occasion). Many prominent and security conscious organizations have decided to focus their energy to consistently addressing what is published on a list such as this, while merely keeping a watchful eye on other issues. There has been a generally positive response from the security community regarding this approach. While this method may prevent over 90% of attacks from occurring, it still may not mesh perfectly with every organization's risk assessment.

Whatever methods are used, such as rapidly responding to periodic network scanning tools or following a list of the current top 10, one thing needs to change. Users and administrators must become educated to the fact that placing any device on a network without first considering the security implications is a very bad practice and can simply no longer be acceptable. With all of this said, if you have determined that printer security is something to seriously address right now, what should you do?

First, a printer manufacturer's history and/or current stance toward security should be deeply considered before purchasing new or replacement models. Many have been doing an extremely poor job, and some have been improving significantly, so do some homework. Remember the "backdoor" example? After it was discovered, rather than improving on this weakness, the manufacturer simply changed the hidden URL, which was once again discovered. Worse, the previous vulnerability could be fixed by turning off the web server, but apparently this option has now been disabled. Some manufacturers, on the other hand, have been addressing problems quickly and providing useful documentation to help configure printers securely. HP, for example, has produced a helpful document called "Making HP Jetdirect Print Servers Secure on a Network."

There are a number of things that can be done to strengthen the defenses of printers currently in use. Most importantly, make sure that the network is protected by decent firewall hardware and that it is configured according to a default-deny policy.

Next, make sure the firmware stays up to date. This can be a daunting task if there are a lot of devices to administer. Fortunately, some manufacturers have made progress in this area. There is a free firmware monitoring tool from HP that will find all of the HP printers on the network, display their current firmware versions, and then allow them to be upgraded.

Unused and/or unsecure services and protocols should also be turned off. If there is a safer way for users to print and admins to administer, then specify only those options as available and turn off everything else. Just remember that if the preferred configuration method is compromised, an attacker can easily re-enable those other less secure services and protocols.

For all the services, be sure to change the default passwords. This should be a strong password, but NOT the same password used for other systems on the network. It has already been shown that there may be some methods for an attacker to potentially read that password, and almost exclusively, the password must be transmitted over the network in clear-text; whereas passwords for securely-configured computer systems would often be protected.

If the device can utilize an access control list (ACL), then make sure it is being used. An administrator could, for example, specify a range of IP addresses that are allowed to connect to the printer.

**Conclusion**

We have seen that there are indeed some things to consider regarding the subject of printer security. There are a few documents in circulation that basically reveal the common threats and vulnerabilities against printers, as does this one. Most, however, tend to make it sound as if the world will end if these are not fixed right now! Some organizations press the panic button when their favorite network scanning tool dumps a load of printer vulnerabilities in their lap. I have tried to emphasize that there are priorities to consider and effective, organized methods to approach a problem without pushing the panic button. The key is to efficiently use resources by analyzing the most critical threats to the organization and then tackling any vulnerabilities that may allow those threats to occur. After careful analysis, printer insecurities may not be a critical enough threat to the institution to immediately dedicate support personnel to address them. But notice the words “after careful analysis.” At the same time, printer security must not continue as it has; an almost completely neglected subject.

What we then come to is perhaps the most unfortunate conclusion to all of this. Yes, some form of printer security is usually necessary simply because of the world we live in and the nature of some people to conceive of increasingly sophisticated techniques to steal information that is not rightfully theirs. Today, information means power and wealth and can affect many people. This results in the necessity to deeply consider security for any and all devices that can display that information. This is especially true for devices on a network. We are being told to prepare for an ever increasing influx of information collecting and disseminating devices. What will be the next successful method of displaying information in the future? Will we have learned to not take security for granted when it is developed? Will we have applied basic security principles to its implementation in our environment? A good way to answer this question is to look at the current procedures for placing devices, such as printers, on your network.

## References


Andress, Mandy. "Printer Protection." 29 March. 2002
URL: http://www.infoworld.com/article/02/03/29/020401opsecurity_1.html
(19 May. 2003)

Backman, Will. "HP JetDirect JetAdmin Password Vulnerability." 1 Aug. 2001
URL: http://www.securityfocus.com/bid/3132/discussion/ (19 May. 2003)

Felteau, Doug. "Securing Embedded Network Devices." 23 Feb. 2003
URL: http://www.giac.org/practical/GSEC/Doug_Felteau_GSEC.pdf (30 April. 2003)

FX and kim0. "Attacking Networked Embedded Systems." Black Hat USA 2002 Briefings and Training.
URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-phenoelit-network.pdf (30 April. 2003)

Ittersum, Shawn, "Vulnerability Note VU#377003." 6 Aug. 2002
URL: http://www.kb.cert.org/vuls/id/377003 (19 May. 2003)

Mattison, Dennis. "Network Printers and Other Peripherals – Vulnerabilities and Fixes." 27 April 2002
URL: http://freshmeat.net/articles/view/445 (15 April. 2003).

Mattison, Dennis. "Printer Vulnerabilities and Exploits"
URL: http://members.cox.net/ltlw0lf/printers.html (15 April. 2003)

Nash, Paul. "SNMP vulnerabilities." 14 Feb. 2002
URL: http://archives.neohapsis.com/archives/ntbugtraq/2002-q1/0106.html
(30 April. 2003)

No author. "HP Jetdirect Print Servers – Making HP Jetdirect Print Servers Secure on a Network."
URL:http://h20015.www2.hp.com/en/document.jhtml?lc=en&docName=bpj05999 (15 April. 2003)

No author. "Controlling Printer Access." 1999
URL: http://developer.intel.ru/download/network/pdf/printer_access.pdf
(24 April. 2003)

No author. "How To Eliminate The Ten Most Critical Internet Security Threats." 25 June. 2001
URL: http://www.sans.org/top20/top10.php (19 May. 2003)

No author. "The Twenty Most Critical Internet Security Vulnerabilities." 3 March. 2003
URL: http://www.sans.org/top20/ (19 May. 2003)

No author. "SNMPv3." 7 March. 2000
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm (19 May. 2003)

No author. "SANS Security Essentials II: Network Security Overview." 2002

Rikarts, Andrew. "Printer Security Essentials." Feb. 2002
URL: http://www.giac.org/practical/Andrew_Rikarts_GSEC.doc (24 April. 2003)