

Praxis Profiline, 2006/03



## Better safe than sorry

*Print data is often at risk*

*Print data can be vulnerable to attack, because networks often lack adequate security mechanisms.*



*Printers do not have to be locked up in a safe. Vital company data can be easily protected while information is being printed.*

Bernd Hausmann

Original paper copies of important company documents are normally stored in locked cabinets. The documents are usually saved in password-protected directories on servers or in electronic archives. However, basic security principles are often violated when the data is transmitted on a network. Print data can contain sensitive company information, and it is often transferred thoughtlessly without any protection in thin client networks. This makes easy pickings for hackers.



Bernd Hausmann is Director Consulting Services at ThinPrint GmbH, Berlin, Germany  
[www.thinprint.de](http://www.thinprint.de)

Companies invest a lot of manpower and money into firewalls, passwords and digital signatures to shield data on their networks and their thin client environments from unauthorized access. For some unexplainable reason, little attention has been paid to one security gap. Print data is often not encrypted when it is sent across a network, and in many cases the data contains clear text. Even persons with relatively modest IT skills can easily access or manipulate the data. Print data is always vulnerable to attack when it is not encrypted for transmission on a network or to an enabled printer. It is also risky to send unencrypted data via WAN links which are often used in thin client computing.

### Employees as a risk factor

It may sound hard to believe, but a number of studies have shown that most hacker attacks and other criminal activities are

carried out by persons who work inside the company and not by anonymous outsiders.

Price Waterhouse Coopers published a study on *white-collar crime* in 2005. At half of the companies which were victimized by white-collar crime, the perpetrators were company employees. The list of motives for staging hacker attacks included attempts to gain personal advantage, business espionage, inquisitiveness, personal satisfaction on the part of hobby hackers, blackmail, sabotage intended to damage the company and mobbing. The attacks always had a negative effect on the companies involved including damage to the company image, competitive disadvantages or legal consequences. In its *Insider Threat Study*, the US Secret Service working along side of the Computer Emergency Response Team (CERT) investigated 23 security attacks that had their origin in company networks. The results showed that 78 of the

attacks were launched by authorized users who had active accounts. The motivation in most cases was financial. In incidents which affected banks and financial service providers, damages exceeded \$500,000 in thirty percent of the cases.

### External attack

External attackers also pose a risk. Hackers attempt to circumvent all of the security barriers in order to penetrate a thin client environment and intercept information including print data. Companies which send data to field offices, clients or suppliers via insecure DSL Internet connections are equally vulnerable. When companies use this method of transferring sensitive data, print data becomes one of the softest targets if not the softest target. Unfortunately, printing does not seem to be a major consideration in most security strategies.

Praxis Profiline, 2006/03



### Print data is easy to hack

To understand just how vulnerable print data is, it is worth taking a look at the print process. When a print job is started, the data is converted into a language which the printer can understand, usually *PCL (Printer Control Language)* or *Postscript*. These languages describe the format and content of the pages of the print job for the printer to interpret.

*Sniffer* programs (some of which are available for free on the Internet) can copy the data from a print job. Other applications, which are also easy to obtain, are used to display the data, allowing a hacker to see a reasonable replica of the original documents on the screen. Agent software such as *ARP spoofing/poisoning* or *DNS poisoning* can redirect print data from other clients to the sniffer, exposing entire networks to surveillance, and criminals can have a field day. They can use an editor to modify original data and then print it using the Windows LPR command. Standards protocols including *LPD/LPR/Sockets* and *SMB/CIFS* do not offer any protection because the data is not encrypted.

### Encryption and certificate management

To provide adequate protection in a thin client environment, it is absolutely essential that print data is encrypted. Version 6.2 of *ThinPrint's .print* solution now offers 128 bit SSL encrypted print data transmission in addition to data compression and bandwidth management. This is the same encryption method that is used in the banking industry. Certificate management should also be used to ensure that print data only goes to trusted recipients and is not redirected. The *ThinPrint* solution employs a *handshaking* mechanism to make sure that encrypted data is only delivered to clients that have a valid certificate. The certificates can be obtained from a root certification authority, or the company can generate them internally. Any terminal unit which has free *.print client* software can decrypt the SSL data stream which is needed to generate the output. If network printers are



**Sophisticated encryption technology provides effective protection for printers which handle SSL print data in thin client networks.**

installed, various devices or the TPG60 gateway can be used. This appliance with integrated *.print* client supports SSL encryption as well as the solution's core functionality including print data compression and optimized bandwidth management.

### Printing in a WLAN

There are additional security risks relating to system access and protection of print data in environments that use a wireless LAN. To prevent unauthorized access to the network, everyone should use solutions which comply with the latest security standards such as *WPA/WPA2*. This technology is much more secure than its predecessor, which was cracked a long time ago. Print servers using *Wi-Fi Protected Access (WPA and WPA2)* are a good alternative. Dynamic keys and authentication give users added peace of mind.

If the WLAN network is well protected from external attack, intruders from outside the company will not be able to access print data. However, the situation is

different for employees who have access to the thin client system. Since these persons have access to unencrypted data, it is advisable to use SSL encryption.

### Other ways of protecting data

In addition to the protection mechanisms listed above, a number of manufacturers offer authentication right at the printer, which ensure that only authorized users will be able to get a printout or will even be able to start a print job. Authentication can be based on biometrics or entry of a user ID and/or a password. Other companies supply physical security products such as lockable cases and stacks which provide physical protection against unauthorized access.

Security starts with employee behavior. There is one security lapse which you will find in nearly every company. Printouts often lie in a printer for hours, giving curious colleagues and employees who have no need to know the opportunity to browse through sensitive information.

Departments that handle sensitive information such as Personnel and Finance should never leave their printouts unattended at a central printer in a thin client network. The better solution would be to ignore the cost and install a printer in the department to print documents which can contain confidential information. This gives better protection from prying eyes.

Printing is no different from any other aspect of IT. There is no such thing as 100 percent security. No company can afford to be complacent. If you want to protect yourself from attack, you would be well advised to remember printing when you are putting together a security strategy for your thin client network. ■



A typical gateway which can be used to protect data in a thin client network.