

Network Computing (UK) May/June 2006

Network Computing



Your print data: is it secure?

Clicking on the "Print" icon does not seem like the most risky network activity - yet it could be. Steven Jones, Technical Consultant at ThinPrint UK explains

Whereas original documents are often carefully protected in closed filing cabinets or password protected directories, print data containing confidential or sensitive information is often unprotected and sent over a network without a second thought. However it is precisely this data that is easy prey for hackers.

Firewalls, passwords, digital signatures - companies invest a lot of manpower and money to protect their data against unauthorised access. Inexplicably, though, little regard has been paid to one security leak: print data, which is sent through the network, is usually unencrypted and often contains clear text. It is therefore relatively easy to crack, or even manipulate, even for technical lay people.

THE TARGETS

Basically, any unencrypted transfer of print data to a network or shared printer, offers opportunities for hacking. Unencrypted transfer of data across a WAN connection is an additional risk.

EMPLOYEES AS SECURITY RISK

The majority of all hack attacks or white-collar crimes are not committed by anonymous culprits outside the company, but come from within the

company itself. This trend is confirmed by the "White-collar Crime 2005" study conducted by Price Waterhouse Coopers. In half of the companies that were victims of white-collar crime, the perpetrators came from within the company's own ranks. The list of hackers' motives ranged from creating personal advantages and corporate espionage, to curiosity and envy of hobby hackers on down to blackmail and corporate sabotage.

In all cases, the attacks were conducted at the expense of the company. Results include a damaged corporate image, competitive disadvantages, and possibly legal consequences. The US Secret Service worked together with the Computer Emergency Response Team (CERT) on its "Insider Threat Study" to study 23 security attacks that originated within corporate networks. The results: 78% of the culprits were authorised users with active accounts. The majority of the perpetrators were pursuing predominantly financial interests. In companies from the banking and financial services sector, damages in 30% of the cases exceeded 500,000 US dollars.

ATTACKS FROM OUTSIDE

Obviously, another risk is external hackers, who infiltrate the network and intercept data, including print data. Also

at risk are companies that send their data to remote offices, customers, or suppliers across unsecured DSL internet connections. In these environments, print data is an easy, if not the easiest, target for acquiring sensitive data.

Unfortunately, the print infrastructure is given no consideration at all in most security concepts.

PRINT DATA IS EASY TO HACK

To understand how vulnerable print data is, one must first visualise the print process. If a print job is started, the data is converted to a language that can be interpreted by the printer. This print command language is usually either PCL (Printer Control Language) or Postscript. These languages describe the setup and content of the individual pages of a print job for the printer. Using so-called sniffer programs, which can even be found for free on the internet, it is possible to record the data of a print job.

If another, equally easily accessible, application is used for displaying the print data the hacker can view more or less the original document on his screen. Agent software like ARP spoofing and poisoning or DNS poisoning, which forwards the print data from other clients to the sniffer, can be used to tap entire networks.

Furthermore, we all know that criminal energy has no limits. Using an editor, the

Network Computing (UK) May/June 2006

Network Computing



original data can also be modified and then printed with Windows own LPR command. Conventional print protocols like LPD/LPR/sockets or SMB/CIFS offer no protection here because they do not enable encryption.

THE ESSENTIALS: SSL ENCRYPTION AND CERTIFICATE MANAGEMENT

One measure is absolutely necessary for safeguarding print data: encryption of the print data stream. Manufacturers and developers are therefore building encryption algorithms into their existing solutions. For example, in addition to its most important functions - print data compression and bandwidth control - the print management solution of the manufacturers, like ThinPrint, offer 128-bit SSL encryption for print data transmission, an encryption algorithm also used for sending back data.

To ensure that the print data is not redirected and only delivered to trusted recipients, an additional certificate management should come into play. With a well designed solution, a so-called handshake system ensures that encrypted data is only sent to clients with an authorised certificate. The required certificates can either be issued by a trusted certificate authority or created by the company itself. Decoding of the SSL data stream, which is necessary for printout, can be performed by any end

device, like a PC, that is furnished with the free .print Client software. If network printers are installed, devices such as the ThinPrint Gateway TPG60 from SEH Technology can be used. This appliance, with an integrated .print Client, not only supports the SSL encryption of the .print solution, it also supports the core functions like print data compression and optimised bandwidth usage. Moreover, the network print specialists at SEH also offer other hardware solutions that transfer print data encrypted all the way from the server to the network printer.

PRINTING IN A WLAN

Architectures with a wireless LAN offer further points of attack, regarding both access to the system and the security of print data. To prevent unauthorised parties from infiltrating the network, companies should in every case apply the latest security standards like WPA/WPA2, which are much safer than its long-ago cracked predecessor, WEP. Help here is found in print servers that are equipped with the encryption methods of WiFi Protected Access (WPA and WPA2) and ideally also ensure additional security with dynamic keys and authentication.

If the WLAN network is outwardly shielded, the print data is also inaccessible to outsiders. Inwardly, though, the situation is somewhat different. Employees with access to the

system can access unencrypted print data. Therefore, it is also recommendable to apply SSL encryption in a WLAN.

OTHER SECURITY MEASURES

In addition to the above security mechanisms, various manufacturers offer solutions for authenticating printers to ensure that only authorised users receive or can even initiate a printout. There are biometric systems as well as the input of a user ID and password. Additionally, there are manufacturers of physical safeguards with which printers are protected by lockable housings or stacks.

At least one security leak can't be blocked, though. How often do printouts lie for hours in the printer, revealing information to curious colleagues whom it doesn't concern? Departments with sensitive information, like the human resources division, should therefore not forget their documents in the printer. It would be even better if they could print their documents from their own printer, to which unauthorised people have no access.

Although there will never be absolute security with printing, as in other areas of IT, no company should allow itself to be careless when dealing with print data. Anyone who wants to be protected against attack is well advised to remember printing in their security concept.