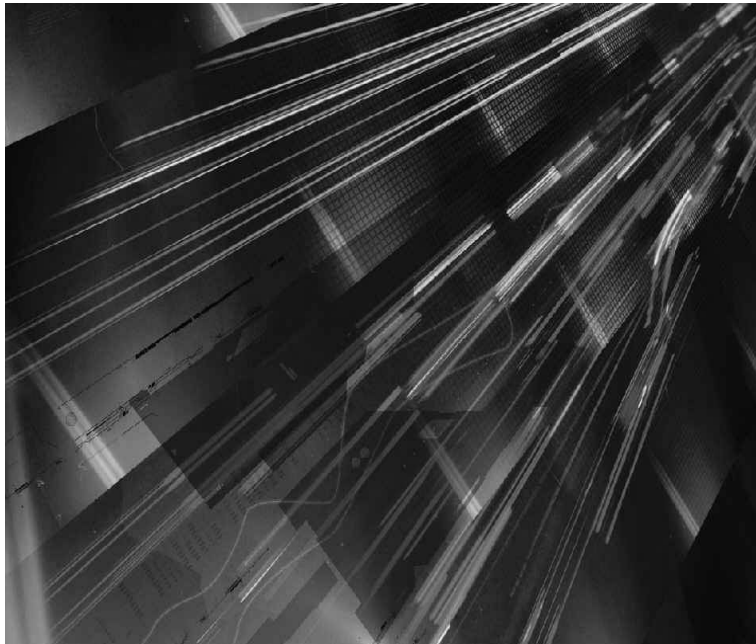

Securing Network Print Jobs

Enterprise Output Management Series



LRS® White Paper



Recently LRS asked one of our Systems Engineers to attempt to capture a print job from our corporate LAN using software and information that would be available to an average individual in most companies. Our goal was to determine just how easy it would be for most users to capture a print job and extract sensitive information from it.

What we learned was shocking—in less than an hour, the engineer downloaded network monitoring, or “sniffer,” software from the Internet, installed and configured it on a PC, used it to capture a print job from our mainframe containing check images, and altered a check amount. The engineer then sent the altered data to the original destination printer and produced a physical check.

While this example illustrates the financial risk of an individual altering the amount of a check, our engineer could just have easily captured and viewed an HR or payroll report, or a document containing confidential patient data. In view of the current laws concerning data privacy, the risks of exposing sensitive personal information are often far greater than the financial loss associated with altering a check – and less likely to be discovered until there is a big problem.

Is It Possible?

Is it really possible for an average PC user to accomplish this feat? Our engineer explained that only three things were necessary for him to capture print jobs from our corporate IP network: A PC connected to the network; the IP address of the target printer; and network monitoring software.

How many individuals have access to those items in today’s typical company? Most, if not all. Networked PCs are standard business tools; many organizations attach labels to their printers showing the IP address for quick identification by network support personnel; and network monitoring software can be downloaded free from the Internet. Because Internet access is nearly as common as telephone service for the majority of today’s employees, many of them have the complete network print job capture toolbox within easy reach.

IP’s Open Nature

The open nature of IP, or Internet Protocol, helps make capturing print jobs the easy task that it is. IP manages the flow of data from the originating system to the data’s destination. First IP breaks a large volume of data, such as a print job, into manageable packets and sends the packets onto the network. Each packet finds its own way across the network; there is no predetermined path for network traffic. When a packet arrives at an IP router, the router decides where to send it next. Because routers can send packets along the path of least resistance, IP traffic often reaches its destination by a roundabout path instead of a straight line. Along its path, a packet is readable by every router and network node it encounters.

Packet sniffing software, also known as network monitoring software, can look inside the packets to see where they originated and what their destination is. Most sniffers can be set to capture all packets marked for a specific destination, such as a network printer. That’s why the printer’s IP address is necessary for capturing print jobs.

Sniffing software provides a legitimate business benefit for network managers by enabling them to view network traffic and diagnose any problem areas. To provide a diagnostic tool for network managers, Microsoft includes a network monitoring application in its WindowsNT Server software. The sad fact is that many tools designed to provide a benefit can also be misused to any company's detriment, and that's the case with sniffer software.

Sniffers available for free from the Internet, which include Ethereal for Windows, WinDump, PacketMon, and others, can be used for network diagnostics or to capture and read the data contained within print jobs. This screen capture from Ethereal for Windows illustrates just how readable data in a print job can be:

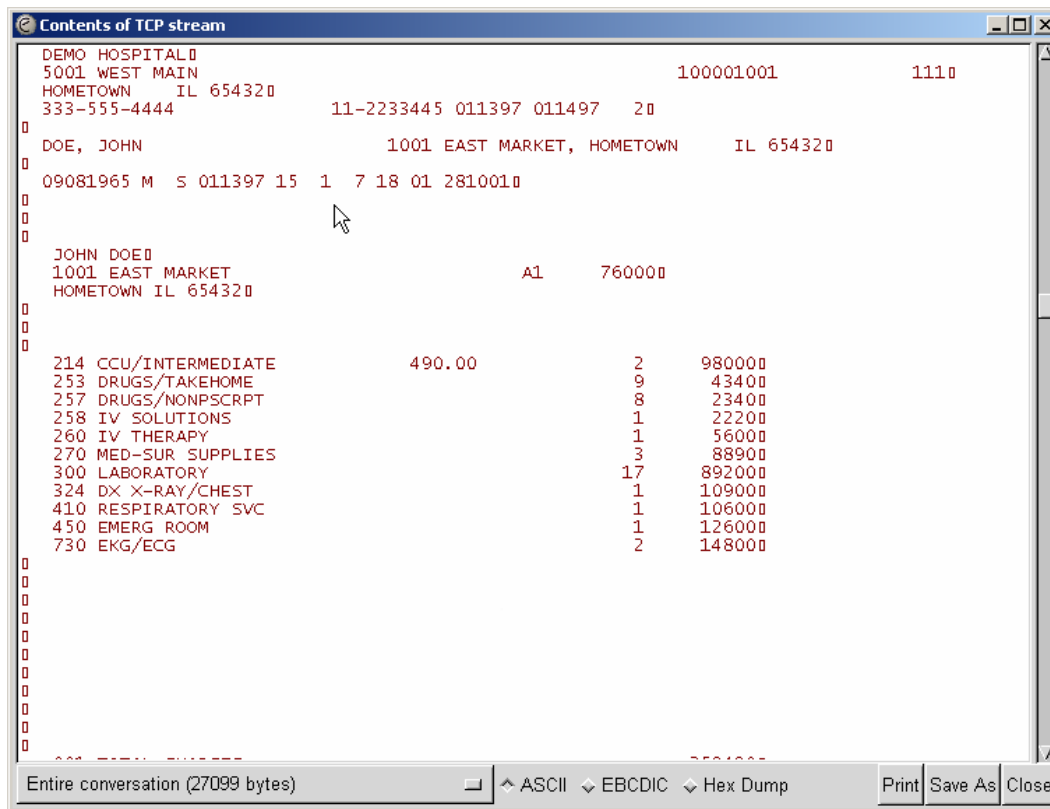


Figure 1—Screen shot of print job captured and read by Ethereal for Windows

As Figure 1 shows, reading the data contained in a captured print job is extremely easy.

Is It Probable?

Although someone working inside an organization really could capture and read or alter print jobs from the internal network without detection, information technology professionals may wonder if such an event is likely. Some sort of internal attack on any corporate network is very likely, according to the annual Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) with the participation of the San Francisco FBI Bureau's Computer Intrusion squad. The 2002 CSI/FBI survey found that 64 percent of all respondents had experienced at least one internal assault on its networks. The remaining organizations didn't know whether they had been hit or not.



Chances are good that their networks had been victimized by someone inside the organization but they simply had not detected the attack. Studies by the CSI, the FBI, and other security experts estimate that 70-80 percent of all corporate data theft occurs inside the organization.

Consider the example of the federal agency which was rocked by the discovery that one of its employees had deliberately defined network print queues that were delivering a copy of sensitive output to printers outside the agency. The agency was completely unaware of this data duplication until a third party conducted a security audit of the agency's networks.

The Limitation of VPN's

Organizations seeking to distribute output securely over shared TCP/IP networks often ask whether it's possible to achieve the appropriate level of security with a VPN, or Virtual Private Network. VPN's are a compelling business solution because they provide high security at a sizable cost reduction compared to a private network.

The most common reason for implementing a VPN solution is to allow remote or mobile users on public networks to connect to the corporate office's private network. The communication flow is encrypted to ensure that only authorized users are able to obtain usable data from the private network.

At first glance, the VPN solution appears to satisfy the requirement for end-to-end secure printing. A closer look reveals that VPN's are concerned only about the *public* segment of the connection, not the total connection between the mainframe application that produces the output and the final destination for the output. The final destination for the output may be a network printer in an open area of the enterprise, for example. As we've already discussed, corporate information can be misused inside the organization just as easily as it can outside the organization.

An article in the January 2003 edition of CSO magazine raises another concern: "The problem with relying on firewalls and VPN, however, is that they encourage poor internal security practices—thinking that the network is safe, administrators don't require the use of encryption for passwords or e-mail. File shares are left unprotected—after all, only people inside the company have access to them, right?"

A VPN should be just one component of an overall network security plan and not the only solution. Along with all the safeguards an organization has implemented to protect internal networks, including firewalls, intrusion detectors, and a VPN, the organization needs to consider security for the print jobs that applications send to network printers.

A Real Threat

Print jobs streaming from any system to network printers or another computing platform obviously face a very real threat. That threat may be an employee armed with free packet sniffing software and the intention to do harm to the organization. The threat may be posed by a simple network routing error.

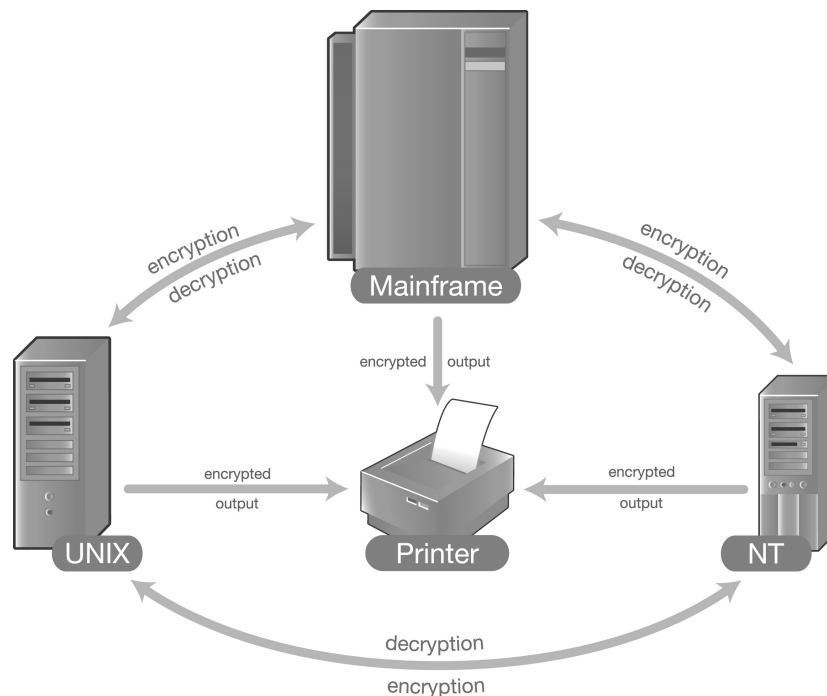
Either way, transmitting print jobs across internal IP networks, shared networks, or the Internet can be risky. Companies need to consider the monetary loss they could incur if proprietary

information, including valuable trade secrets, are intercepted and sold to competitors. Companies also need to consider the potential liability exposure they face if they lose control of confidential employee or other data in print jobs. That’s especially true for organizations that print documents containing information regulated by federal laws such as HIPAA (Health Insurance Portability and Accountability Act) or the Gramm-Leach-Bliley Act.

Financial services companies must protect the confidentiality of customer information to ensure compliance with the Gramm-Leach-Bliley Act. A leading corporation in that field saw the need for additional security for print jobs, although it already had various network security measures in place. The corporation implemented secure printing software from LRS to leverage intranet infrastructure for printout delivery while meeting its commitment to protect confidential customer data. The LRS® solution protects print jobs so well, the company was able to actually use the internet for transmitting print jobs to remote locations without fear of compromising confidential information.

Securing Distributed Output

Providing security for the print jobs streaming from applications to network printers is the purpose of secure software products from LRS. These products are capable of encrypting application output—that is, encoding it so the data is unreadable—for secure transmission over TCP/IP networks to printers or other platforms capable of decrypting, or decoding, the data stream. The result is secure platform-to-printer output delivery or platform-to-platform file transfer.



Because there is no guarantee that VPN’s, switched hubs, Secure Sockets Layer (SSL), Secure Shell (SSH), or other network security measures will prevent someone from intercepting print jobs, the best way to secure the data in those jobs is to encrypt it.

How well do print jobs encrypted by LRS® software hide their data? Consider this example, which is the same print job that we used for Figure 1. This time we encrypted the print job using LRS software before we sent it across our network and captured it using Ethereal for Windows.

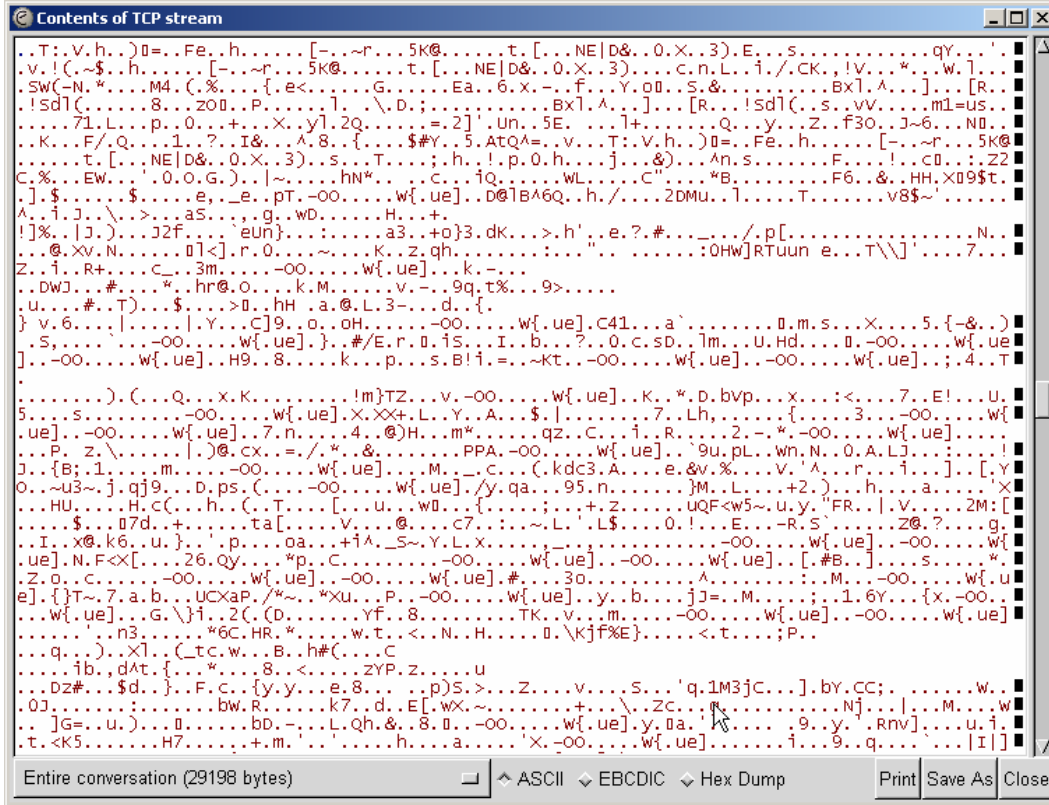


Figure 2—Screen shot of encrypted print job captured and read by Ethereal for Windows

Encryption hides the data contained in print jobs from the mainframe all the way to the destination printer. Anyone who compromises network security and captures or duplicates a print job will be prevented from actually seeing the data the job contains.

Take another look at the federal agency we mentioned on page 3. By implementing the encryption available with LRS software, the agency would have protected its print jobs even if an employee defined network print queues to duplicate and re-direct those jobs. Once the print jobs reached their destinations outside the agency, the recipients would have seen something like the above illustration instead of readable data.

Basic Terms

Encryption and decryption are basic terms in any discussion of computer network security.

Encryption is technology that "encodes" computer files and communications to protect privacy, like the way a combination lock secures a filing cabinet. *Decryption* is the process that decodes files, converting them to a readable form. These processes are part of the science of *cryptography*,



which is the study of methods for transforming information into a form which secures that information while in storage or in transit. Cryptography is Greek for “hidden writing.”

Cryptographers call the readable data—in other words, data that has not been encrypted—*cleartext*. Once the data is encrypted, it’s referred to as *ciphertext*. The secret password or table needed to decipher encrypted data is called the *key*; the right key is therefore required to “unlock” ciphertext and transform it back into the original cleartext data.

LRS® secure software products use the Rijndael encryption algorithm to encrypt and decrypt output.

Rijndael Encryption Algorithm

In May 2002, the United States government adopted the Rijndael encryption algorithm as the Advanced Encryption Standard (AES). Rijndael had been selected by the National Institute of Standards and Technology (NIST) over other algorithms because of its combination of security, performance, efficiency, ease of implementation, and flexibility. NIST found Rijndael to be a consistently good performer in both hardware and software across a wide range of computing environments.

Rijndael enables the user to choose key lengths of 16, 24, or 32 bytes (128, 192, or 256 bits). Generally speaking, the longer the key, the harder it is to break the encryption algorithm. A one-byte key length, for example, provides just 256 possible keys; a seven-byte key length provides about 70 quadrillion, or 70,000,000,000,000,000, possible keys; and a 16-byte key length allows for 300,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 unique keys.

Hardware Decryption

LRS is working with leading printer manufacturers and other hardware vendors to provide secure mainframe output distribution to a variety of devices. There are now solutions available to support printers from Hewlett-Packard and Lexmark International. In addition, Intermate A/S offers a decryption-capable print server which connects to the parallel port of many popular printers and copiers. Additional vendors have solutions in development.

HP

Capella Technologies, Inc., has built a secure printing solution, the SecureDIMM II, which installs directly into one of the memory expansion sockets of selected HP printers. The SecureDIMM II firmware is executed by the printer’s microprocessor to utilize decryption capabilities. The SecureDIMM II is available for HP LaserJet 4200, 4300, and 9000 printers; HP Color LaserJet 5500 printers; 4100MFP and 9000MFP printers; and other recent models on request.

Intermate

Intermate 100 and 101 print servers support the Intermate Secure Print Protocol (ISPP), which can decrypt ciphertext received from LRS® secure software. To provide secure end-to-end document delivery, the Intermate print server must be connected to a printer that supports bi-directional communication and PJJ commands.



Capella's SecureDIMM II and Intermate's print servers use static, or persistent, keys for decrypting print jobs they receive. LRS software is configured to encrypt all the jobs it sends to one of these devices using the same key each time.

Lexmark

Lexmark's secure printing solution is unique in offering the capability to generate dynamic session keys for every print session. The Lexmark PrintCryption™ Card, which fits the company's T series printers, generates a new key when VPS/Secure™ alerts it that a print job is coming. Once the job has printed, the encryption key expires.

An analysis of Lexmark's PrintCryption Card, written by CAP Ventures, Inc., is available on the Web at this site:

http://www.lexmark.com/US/products/networking/printcryption/Lexmarks_New_PrintCryption_by_CapV.pdf.

Like secure software from LRS, these hardware products utilize the Rijndael encryption algorithm. Using these printers along with the LRS solution on the mainframe, an organization can obtain the benefits of secure printing and page-level confirmation. Bi-directional Internet Printing (BIP) support in LRS software provides confirmation that each page of the encrypted print job has actually been printed.

LRS software encrypts output as it is captured from the MVS JES spool or applications on UNIX or NT servers and routes it over TCP/IP networks to a specific decryption-capable printer which interprets the encrypted data stream, decrypts it, and enables the printer to produce readable final documents. Intercepted output will not print on any other device.

Conclusion

Shared TCP/IP networks like the global Internet offer organizations a low-cost alternative to leased lines and other forms of private network infrastructure for distributing print jobs to various locations. Whether they are transmitted across public shared networks or an internal network, print jobs represent a vulnerable type of network traffic.

Print jobs are formatted to be easily read before they are transmitted and represent a security exposure that most organizations have simply not considered. Any print jobs that include sensitive, confidential, or mission-critical information need to be secured from the application that generates it to the device that prints it.

LRS® secure software offers organizations a reliable method for achieving end-to-end security over network printing. Jobs can be encrypted where they are created and decrypted only at the destination where documents are produced.

Learn More

For more information on secure network printing using LRS software and a variety of hardware devices, visit our Web site: www.vps.com/GENSecure.asp.



About LRS

Levi, Ray & Shoup, Inc., is the industry leader in Enterprise Output Management products—our software runs on more than 5,000 Enterprise systems worldwide. Founded in 1979, LRS is now an information technology firm of 500 employees offering a variety of products and services. We developed the first software that enabled the MVS mainframe to distribute output to printers outside the data center, and today our Enterprise Output Management family of software products provides output distribution, data stream conversion, monitoring/control, and viewing/archiving throughout an enterprise.

For additional information, contact:

Levi, Ray & Shoup, Inc.
2401 West Monroe Street
Springfield, IL 62704
(217) 793-3800

www.vps.com or email questions to asklrs@LRS.com