April 2005 Vol.7 No.1

LINK

Lava I/O News

Inside this issue:

IP-Enable Legacy Payment Terminals

How many times have you stood at a checkout line and listened to the merchant's modem dial out to process your credit card or debit card? This common scenario is becoming a thing of the past, as payment transaction processing moves from conventional telephone lines and modems to IP-based Internet connections.

Advantages of IP-based transaction processing

The move to IP-based transaction processing makes a lot of sense for both payment processors and merchants, not to mention its benefit to everyday consumers. From the standpoint of the organizations who receive the credit card, debit card, or loyalty card requests (let's call them the "payment processors"), moving such transactions to IP means they no longer need to maintain a vast pool of modems and phone lines. Such setups have required the payment processors to invest heavily in a telephony infrastructure geared to handle peaks in demand, but that infrastructure is overbuilt for day-to-day needs. The number of transactions being processed at any time can vary greatly, from the peak of a pre-Christmas buying spree to a lull in the small hours of the morning in April or May.

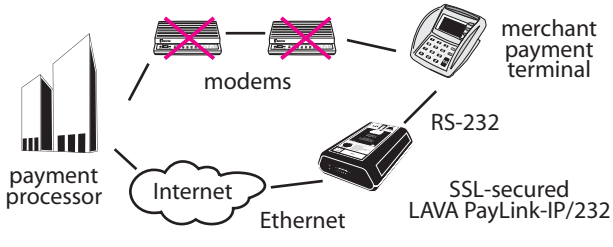
With IP payment processing, the costs of infrastructure and communications lines are greatly reduced. An IP connection can handle many transactions virtually simultaneously; by contrast, a telephone line is generally able to handle just one transaction at a time.

For the merchants too, advantages arise in moving payment processing to the Internet. Foremost among these is reduced transaction times: a modem takes considerably longer to dial up, connect, and transmit a transaction's information than does a network-based system. Although the amount of data being sent in any transaction is minuscule, the time taken for a phone line to open as a modem connection is significant. Customers standing in checkout lines and hearing the modem dial up and complete its screechy negotiation with a remote modem have painful evidence of how that time is spent. And what vendor wants to have cashiers standing around while checkout lines grow longer?

A second advantage to many merchants is that they can free up or even totally eliminate a phone line. Merchants who process transactions across the same phone line they also use for voice or fax transmissions, will see the competition between uses of the phone line vanish. Merchants who have a dedicated phone line for payment processing may be able to eliminate that phone line altogether, if they already have Internet access for other purposes.

Not a free transition

The advantages of switching to IP-based transaction processing do not however come without a cost. Between the merchant with existing payment terminals (terminals that either use a modem or have a modem built in),



LAVA PayLink-IP/232 eliminates modems for payment processing

IP-enable legacy payment terminals (continued)

and the payment processor with their own modems, somebody needs to pay for the change in infrastructure needed to realize the benefits of moving payment processing to IP. This cost is usually split in some fashion between merchant and payment processor, with the payment processor sometimes offering inducements to merchants to make the switch. Such inducements could be reduced rates charged for payment processing, or discounted pricing on new, IP-ready payment terminals. Despite the advantages to the merchant of networked payment processing, the expense of replacing outmoded payment terminals might outweigh the savings, particularly in the short run, if the full cost must be borne out of pocket.

Here is where Lava comes in. Lava's PayLink-IP products are the ideal secure communications link for cost conscious merchants and payment processors. With a PayLink-IP, existing payment terminals can be transparently converted to become networked devices, at a fraction of the cost of a new terminal. This cost savings benefits everyone.

LAVA's cost-effective solutions

For merchants using payment terminals that can output transaction data through a serial port to a modem, the LAVA PayLink-IP/232 is the solution. This device takes the data that would normally be sent to the modem, and transparently sends it across a network connection to the payment processor. All of this is done securely and transparently – no changes need to be made to the POS software or hardware.

LAVA PayLink-IP/232

LAVA PayLink-IP/Dial

Merchants whose payment terminals have built-in modems that plug directly into a telephone jack also have a solution: the LAVA PayLink-IP/Dial. From the point of view of the payment terminal, the LAVA PayLink-IP/Dial looks exactly like a telephone line, complete with RJ-11 wall jack. This device takes the output from the payment terminal's modem and, like the LAVA PayLink-IP/232, transparently sends it across a network connection to the payment processor.

In both cases, the essential difference is that the connection used for the payment processor is now an IP address, instead of a telephone number. Both the PayLink-IP/232 and the PayLink-IP/Dial have configuration screens that allow merchants to enter the IP addresses needed to connect to their payment processors. It's that simple.

LAVA's secure connectivity

Network connectivity is fundamentally different from the type of connection created by a modem-to-modem link on a phone line, and this difference has significant implications for security. TCP/IP, the method of networking on the Internet, has a structure that needs supplementing to be truly secure for the purpose of transmitting financial transaction information. Lava has implemented 128-bit version 3.0 SSL on its PayLink-IP products to ensure security that meets the standards required by today's financial community.

The Ether-Serial Link product line grows

When connecting serial devices to an Ethernet does not require the high-level security of SSL, conventional serial device servers serve extremely well. Lava's line of Ether-Serial Links are designed for these applications, whether you are connecting factory equipment to a LAN, POS equipment to the Internet, a data logger to a WAN, or any other type of serial connection.

Lava's Ether-Serial Links now include versions with one, two, four, and eight ports, in RS-232, 422, and 485 configurations.

What is SSL?

SSL (Secure Sockets Layer) is a protocol for establishing a network connection (a "socket") that is secure enough to transmit sensitive data. In the case of the LAVA PayLink-IP, SSL is the security protocol used for transmitting financial transaction information over a connection established between an SSL-enabled client and an SSL-enabled server (specifically, between the LAVA PayLink-IP and the payment processor's SSL server).

SSL originated with the Netscape browser, as the need arose for a secure means for web users to interact with web sites and their web servers. When browsers were simply used to passively view web pages, there was no need for SSL. But as users of the Internet began buying and selling things online, the need for greater network security became apparent. Today, SSL is the usual standard accepted as suitable for secure data transmission.

SSL has evolved since its early implementations, and the version 3.0 128-bit SSL used by the LAVA PayLink-IP/232 and the LAVA PayLink-IP/Dial has no known vulnerabilities. SSL ver. 3.0 is the most widely-implemented version and will remain so for some time, but SSL continues to evolve, with TLS 1.0 (Transport Layer Security), also known as SSL version 3.1, now developed by the Internet Engineering Task Force (IETF) as an "official" standard (RFC 2246).

SSL establishes a framework for encryption to work within, but is not in itself primarily concerned with encrypting data. While a full description of SSL's operation is beyond the scope of this newsletter, a simple overview of the protocol will nevertheless help to give some sense of what is going on when a client and server set up an SSL connection.

Basically, when an SSL client (a LAVA PayLink-IP) contacts an SSL server, the client and server initially exchange information about their SSL version numbers, the cipher key types they will use to set up the connection, and some initial data to be used in deriving cryptographic keys. The cipher keys are used in the SSL session to authenticate the client and server to each other, to transmit certificates, and to establish session keys. The SSL server sends its "digital certificate," which the client verifies against a set of criteria for acceptance (X.509 certificates are used in standard SSL implementations).

When generating a certificate the server sends an unencrypted "public key" to the client and generates a private key for itself. Since the public key is unencrypted, the server, the client, and any potential eavesdropper can read the key. The client receives the public key and generates a quantity of random data (called the "pre-master secret") using a public-key cryptography standard (PKCS#1). It then uses the public key received from the SSL server to encrypt this number and send it to the SSL server. The SSL server, with its private key, is the only other system that can determine the client's secret number. This number becomes the basis for generating the "master secret," which in turn is used to create a set of cipher keys that are used to encrypt the rest of the session between the client and the server.

SSL also defines how a connection is securely closed, what constitute violations of its security model, and additional security features. The result of all of this cryptology is technology that enables the LAVA PayLink-IP to establish a secure link with a payment processor's server – just what is needed for processing financial transactions.

REFERENCES

- http://www.freesoft.org/CIE/Topics/121.htm [Overview of SSL and TLS]
- http://www.openssl.org/docs/crypto/rc4.html [Open-source cipher compatible with RC4™, proprietary RSA Security Inc. cipher]
- http://www.openssl.org/related/ssl.html [Links to documents on SSL and TLS, and public-domain SSL source code]
- http://www.ietf.org/rfc/rfc2437.txt [IETF RFC 2437 – PKCS #1: RSA Cryptography Specifications Version 2.0]
- http://www.ietf.org/rfc/rfc2246.txt [IETF RFC 2246 – The TLS Protocol Version 1.0]
- http://www.ietf.org/rfc/rfc2459.txt [IETF RFC 2459 – X.509 Certification]
- http://www.treese.org/ietf-tls/ [IETF Working Group on Transport Layer Security]

Upcoming Shows

Lava will be attending the following shows in the next month:

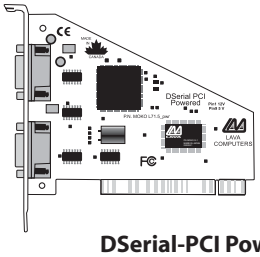
Retail Systems 2005
Chicago, Illinois
May 24-26
Booth 1441

National Restaurant Association 2005
Chicago, Illinois
May 21-24
Booth 2192

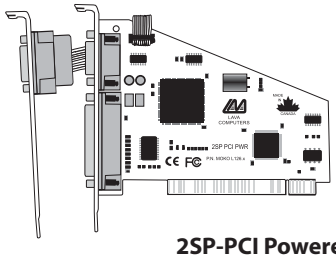
We'd love to see you at one of these shows!

Next issue: Powered Serial Ports

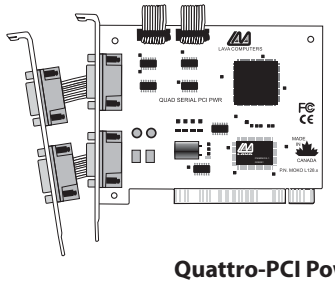
Lava has introduced a line of serial port boards that provide power to serial peripherals across the serial port connector. Next issue of LINK will look at these boards and the advantages they offer.



DSerial-PCI Powered



2SP-PCI Powered



Quattro-PCI Powered

LAVA ETHER-SERIAL LINK DEVICE SERVERS

	Ports					Connectors			Modes			
Product	**1**	**2**	**4**	**5**	**8**	**DB-9**	**RJ-45**	**Powered**	**RS-232**	**RS-422**	**RS-485**	**TTL**
Ether-Serial Link 1-232-DB9	✔					✔			✔			
Ether-Serial Link 1-232-RJ45	✔						✔	✔	✔			
Ether-Serial Link 1-422-DB9	✔					✔				✔		
Ether-Serial Link 1-485-DB9	✔					✔					✔	
Ether-Serial Link 1-TTL	✔											✔
Ether-Serial Link 2-232-DB9		✔				✔			✔			
Ether-Serial Link 2-232-RJ45		✔					✔	✔	✔			
Ether-Serial Link 2-422-DB9		✔				✔				✔		
Ether-Serial Link 4-232-DB9			✔			✔			✔			
Ether-Serial Link 4-232-RJ45			✔				✔	✔	✔			
Ether-Serial Link 4-232-DB9-CBL			✔			✔			✔			
Ether-Serial Link 5-232-DB9-EMB				✔		✔			✔			
Ether-Serial Link 8-232-RJ45					✔		✔	✔	✔			
Ether-Serial Link 8-232-DB9-CBL					✔	✔			✔			

LAVA PAYLINK-IP PAYMENT TERMINAL SERVERS

	Ports	Processor Addressability				Connectors		Modes		Security
Product	**1**	**Credit**	**Debit**	**Config.1**	**Config.2**	**DB-9**	**RJ-11**	**RS-232**	**POTS**	**SSL Ver.3.0 128-bit**
PayLink-IP/232	✔	✔	✔	✔	✔	✔		✔		✔
PayLink-IP/Dial	✔	✔	✔	✔	✔		✔		✔	✔

LAVA BOARD-LEVEL PRODUCTS

Serial Port Boards (PCI Bus)

SSerial-PCI	Single 9-pin serial, 16550 UART
SSerial-PCI/LP	Single 25-pin serial, 16550 UART, low profile
LavaPort-650	Single 9-pin serial, 16650 UART
RS422 SS-PCI	Single 9-pin serial, 16550 UART, RS-422 pinouts
DSerial-PCI	Dual 9-pin serial, 16550 UARTs
DSerial-PCI Pwr	Dual 9-pin serial, 16550 UARTs, 5 & 12 VDC serial power
DSerial-PCI/LP	Dual 9-pin serial, 16550 UARTs, low profile
DSerial-PCI 3.3V	Dual 9-pin serial, 16550 UARTs, for 3.3 volt PCI
LavaPort-PCI	Dual 9-pin serial, 16650 UARTs
Quattro-PCI	Four-port 9-pin serial, 16550 UARTs
Quattro-PCI Pwr	Four-port 9-pin serial, 16550 UARTs, 5 & 12 VDC power
Quattro-PCI/LP	Four-port 9-pin serial, 16550 UARTs, low profile
Quattro-PCI 3.3V	Four-port 9-pin serial, 16550 UARTs, for 3.3 volt PCI
LavaPort-Quad	Four-port 9-pin serial, 16650 UARTs
Octopus-550	Eight-port 9-pin serial, 16550 UARTs

Serial Port Boards (ISA Bus)

SSerial-550	Single 25-pin serial, Com 1-4, 16550 UART, IRQ 3/4/5/7
DSerial-550	Dual 9-pin serial, Com 1-4, 16550 UARTs, IRQ 2/3/4/5/7/10/11/12/15
RS422-550	Dual 9-pin serial, 16550 UARTs, RS-422 pinout
LavaPort-ISA	Single 9-pin serial, Com 1-4, 16650 UART, IRQ 2/3/4/5/10/11/12/15
LavaPort-PnP	Single 9-pin serial, 16650 UART, Plug and Play

Combo Serial & Parallel Port Boards (PCI & ISA Bus)

PCI	SP-PCI	Single 9-pin serial, 16550 UART + single bi-directional parallel
	2SP-PCI	Dual serial (9 & 25-pin), 16550 UARTs + single EPP parallel
	2SP-PCI Pwr	Dual serial (9 & 25-pin), 16550 UARTs + single EPP parallel, 5 & 12 VDC serial power
	LavaPort-Plus	Dual serial (9 & 25 pin), 16650 UARTs + single EPP parallel
ISA	2SP-550	Dual 9-pin serial, Com 1-4, 16550 UARTs + single bi-dir. parallel, LPT 1-2

Parallel Boards (PCI & ISA Bus)

PCI	Parallel-PCI	Single EPP parallel
	Parallel-PCI/LP	Single EPP parallel, low profile
	Parallel-PCI 3.3V	Single EPP parallel, for 3.3 volt PCI
	Dual Parallel-PCI	Dual EPP parallel
ISA	Parallel Bi-dir.	Single bi-directional parallel port, LPT 1/2/3, IRQ 5/7
	Parallel-ECP/EPP	Single ECP/EPP parallel, LPT 1-6, IRQ 2/3/4/5/7/10/11/12

Combo Serial & Parallel Port Boards (PCI & ISA Bus)

PCI	SP-PCI	Single 9-pin serial, 16550 UART + single bi-directional parallel
	SP-PCI Pwr	Single 9-pin serial, 16550 UART + single bi-directional parallel, 5 & 12 VDC serial power
	2SP-PCI	Dual serial (9 & 25-pin), 16550 UARTs + single EPP parallel
	LavaPort-Plus	Dual serial (9 & 25 pin), 16650 UARTs + single EPP parallel
ISA	2SP-550	Dual 9-pin serial, Com 1-4, 16550 UARTs + single bi-dir. parallel, LPT 1-2

Specialty Boards

8255-PIO	8255 PIO interface card, fits in PCI slot
USB 2.0 Host	Dual USB 2.0 ports, 480 Mbps, fits in PCI slot
USB 1.1 Host	Dual USB 1.1 ports, 12 Mbps, fits in PCI slot
FireHost	Dual IEEE 1394 ports, 400 Mbps, fits in PCI slot
FireWire-IDE	FireWire®-to-IDE hard drive interface

Speak to us about your design needs. Apart from the products listed here, Lava customizes and modifies designs to suit specific customer needs.

2 Vulcan Street
Toronto, ON
Canada
M9W 1L2

TEL: 416.674.5942
FAX: 416.674.8262
www.lavalink.com

LIFETIME WARRANTY