CITI Technical Report 95−x

Digest
USENIX Workshop on Electronic Commerce
July 11−12, 1995

P. Honeyman
honey@citi.umich.edu

ABSTRACT

This two-day meeting was organized to foster interaction between the commercial and technical communities engaged in the design and deployment of systems of electronic commerce. Attendance was by invitation from among those who responded to the call for participation. The workshop featured lightly refereed formal presentations, panel sessions, invited talks, and broad, open-ended discussions on technological and social topics.

October 3, 1995

Center for Information Technology Integration
University of Michigan
519 West William Street
Ann Arbor, MI 48103-4943

Digest
USENIX Workshop on Electronic Commerce
July 11–12, 1995

P. Honeyman
`honey@citi.umich.edu`

1. Tuesday, July 11, 1995

Ninety-four attendees were invited to the USENIX Workshop on Electronic Commerce. In his opening remarks, Program Chair Dan Geer set the tone for the conference by requesting that participation be spirited, stressing the urgency of solving electronic commerce problems before the ‘‘cumulative investment’’ of the Internet, more commercial than ever, pins down policies that might wreak havoc with privacy, security, and needed functionality.

1.1. Keynote address

Electronic Banking and Electronic Commerce on the SuperInformation Highway
Daniel Schutzer
Citibank

Dan Schutzer is Vice President and Director of Advanced Technology at Citibank, and President of the Financial Services Technology Consortium. Dan opened his keynote address with an overview of the present information infrastructure for electronic commerce, consisting of the combination of a number of components (*e.g.*, the Internet, telephones, EDI, *etc*.). Continuing to develop at a rapid pace, the resultant information infrastructure may revolutionize the way commerce is conducted. Components are provided by several different industries that need to integrate their products and divide the costs and proüts from the resultant infrastructure.

Dan sees both excitement and fear about achieving wide-scale electronic commerce. Electronic commerce has the potential to break monolithic corporations into smaller, more efücient organizations that buy and sell from each other via the net. Because so much of the net is free, a shift will result in the value-chain between producer and consumer. For example, the net blurs distinction of place, making it no more or less efücient to go inside or outside the company, so in-house design or production departments might bid on contracts just like outsiders.

Electronic commerce involves everything one can do in the physical world: advertising, shopping, bartering, negotiating contracts and prices, bidding for contracts, ordering, billing, payment, settlement, accounting, loans, bonding, escrow, *etc.* Electronic commerce is both a threat and a promise ï it holds the promise of new markets, channels, types of products, and employment, but threatens present jobs and personal security. To reduce these fears, the information infrastructure should provide privacy, protection of intellectual property rights, authentication, authorization, non-refutability, and reliable payment structures.

At the heart of electronic commerce is an act of payment; the information infrastructure implements electronic commerce primarily by implementing that act. Payment can take place in several ways, and many payment methods must be supported. At present, there are lots of players and protocols. Interoperability among different payment systems is critical. Without it, fears about the value of different electronic currencies will scare customers away. With it, the payment process can be automated to reduce costs, which, along with ubiquity of service, can improve customer satisfaction.

Privacy usually implies anonymity, yet the absence of face-to-face social mechanisms for establishing trust exacerbates the difüculty in offering secure and trusted payment systems. And because electronic commerce transactions are several orders of magnitude faster than in the physical world, if it is easy to cheat someone, even for a very small amount, it is easy to do it many, many times over. The costs can add up quickly.

Dan discussed the goals of the Financial Services

Technology Consortium (FSTC), which identiües applications of electronic commerce and guides standards development as the marketplace evolves from a paper-based market to a more electronic-based market. The FSTC is interested in modular standards and open APIs to enable interoperation. Standards development is guided by the principle that new systems should be at least as convenient as current systems, such as ATMs. Electronic currency should be similar in style to an electronic check but provide a wider set of payment options, such as direct funds transfer and payment on credit.

The FSTC established the Electronic Clearinghouse, a system of electronic checks and imaging of paper-based checks. The electronic check system is interesting because there is no need for a transaction-time third party (the bank), yet it is just like a physical check transaction. Plans are to extend the system to cover digital cash, debit cards, credit cards, funds transfer, traveler's checks, barter, *etc.*

The imaging of physical checks allows for faster processing and lower costs. Point-of-sale check scanning combined with online transaction-time veriücation of the account and the amount of the transaction lets the customer tear up the check at the point-of-sale: once it has been scanned, it is never needed again. Fraud prevention and detection schemes need more investigation. Old techniques, such as PINs, may not be adequate in the electronic market because they are hard for users to remember and easy for computers to break. Other techniques, such as neural nets or biometrics (iris scanning, üngerprinting, *etc.*), should be researched. Dan concluded that electronic commerce will likely make life different but more interesting as well.

Jacob Levy opened the discussion by questioning whether humans will trust a system built on intangibles, especially if it includes biometrics. Robert Gezelter expressed concerns about legal ramiücations. For example, what will stand up in court? What if a check image from an imaging system was unclear? Is the user liable? To what extent are Uniform Commercial Code issues being pushed down to the level of consumers? Dan emphasized that many of these questions are current research issues but noted that the consumer's world is already full of risks, such as bad checks or counterfeit cash.

Richard Field responded that consumers and commercial enterprises are in different legal arenas and that the end user is often protected in ways that the commercial enterprise is not. But new proposals are eroding the protections of the consumer. For example, it has been proposed that the liability of the consumer on goods purchased with a stolen credit card be raised from $50 to $500. And scarier, a Utah digital signatures act makes the user liable for credit fraud if digital signatures are used negligently. The problem is that we are applying top-level legal concepts to the consumer.

Lee Parks also noted that the general trend seems to be pushing the risk of fraud onto the consumer. For example, many banks now state that if you have not objected to your monthly statement within 30 days of its issue, all records stand as printed. Many commented on the unacceptability of this trend in the customer community. Dan agrees that there are ''a lot of mineüelds.''

Cliff Neuman commented that people are willing to give their credit card number over the phone to make purchases, so perhaps perfect security is not necessary.

1.2. Economy and legal

Chaired by Alan Nemeth.

Token and Notational Money in Electronic Commerce
L. Jean Camp, Marvin Sirbu, J.D. Tygar
Carnegie Mellon University

Jean Camp presented the ürst formal paper of the workshop. Her thesis is that electronic commerce necessitates new legal and social protocols for handling and processing money. New types of currency pose threats that are not addressed in current law. Jean provides a useful and comprehensive collection of case studies examining the relationship between buyer and seller, as well as the requirements and states of knowledge of law enforcement, banks, and observers, for the various types of electronic currency.

A few questions arose regarding nomenclature, *e.g.*, whether NetBill is goods-atomic. There was also some discussion about the best way to view paper transactions. Greg Rose suggested that the work be extended to address international jurisdictions. Eric Hughes surmised that legislation to prohibit new types of money laundering is inevitable.

Economic Mechanism Design for Computerized Agents
Hal R. Varian
University of Michigan

Hal Varian described issues surrounding economic mechanism design, focusing on auction techniques used in practice and their applicability to electronic commerce. In the discussion, Doug Tygar suggested clever ways to ‘‘hack’’ the auction mechanism. Hal offered a ‘‘mechanism, not policy’’ defense. Jacob Levy explored anonymity in auction mechanisms. Hal responded that the value of anonymity would be reëected in price differences.

Can the Conventional Models Apply? The Microeconomics of the Information Revolution
Bruce Don and David Frelinger
RAND Corp.

Bruce Don argued that the information technology industry is invalidating basic legal and regulatory policies and that there is not yet a clear paradigm that regards information as an economic good.

In the discussion that followed, Hal Varian suggested that we don’t need new economic theories, we just need to read economics texts from the back to the front ï the good stuff is all at the end.

Marvin Sirbu characterized negligible production cost as the key to the economics of software. Dan Schutzer postulated a world of totally free information in which value arises from skillful information management.

Panel Session
Jean Camp, Bruce Don, Hal Varian, Jill Ellsworth

Following brief remarks by Jill Ellsworth, Ph.D., Alan Nemeth led a panel discussion among the authors. Jill is an author, educator, and consultant working with merchants, who are focused more on interoperability than on security. Consumers want systems that are easy, fast, and understandable. Merchants want the system to *work* and they want to get *paid.*

Dan Geer noted a decline in the use of cash, *e.g.*, in grocery stores, replaced by credit or debit cards. ‘‘Do not underestimate the lure of convenience.’’ But how can consumers be protected from unwitting violations of their own interests, *e.g.*, their privacy? Hal Varian feels that they can, with a cost. Bruce Don suggested that we may have the opportunity to design the market mechanisms, which ordinarily form of their own accord. This may allow tailoring speciüc properties of the market, such as those that relate to privacy.

Richard Field described privacy as a commodity to be purchased. Hal Varian characterized it as information of the form ‘‘What does he know?’’

Ittai Hershman questioned whether consumer issues are as important as enterprise issues. Jill noted that business-to-business commerce is well under way, even on the Internet.

Alan Nemeth opened Pandora’s box by suggesting a parallel to the battle between FAX and Email over the last 15 years. More heat than light was shed in response. Much more.

1.3. Payment experience

Chaired by Steve Dusse.

Internet Information Commerce: The First Virtual Approach
Darren New
First Virtual Holdings, Inc.

First Virtual Holdings (FVH), which has been online since October 15, 1994, is in the business of information commerce, not goods and services. Darren New described the problems in supporting electronic commerce on the Internet. The biggest problem is that the Internet is *big.* He also described quite a few ways in which information commerce differs from commerce in real goods. He then described the FVH techniques in some detail.

FVH shies away from cryptographic protocols, which present legal problems as well as potentially interfering with interoperability and usability. In fact, the FVH protocols send no ünancial information over the net.

In answer to Robert Simoncic’s question, Darren revealed that FVH has over 10,000 customer accounts. Darren did not indicate the amount of foreign trafüc or how many users employ non-IP protocols, such as UUCP. In the early days, most of FVH’s business was done through FTP and SMTP; now it’s done mostly via the Web. In response to Marvin Sirbu’s question about microtransactions, Darren indicated that sellers are allowed to accumulate transactions before forwarding billing requests to FVH.

Ben Wright asked about the trust relationship between sellers/customers and FVH. Darren replied that FVH is relying on establishing and enhancing its reputation through presence on the net, 800 numbers, relationships with large vendors, *etc.* Dave Crocker made a strong pitch for reputation-based systems.

Arthur Keller asked how FVH handles ‘‘varying content.’’ This seemed to be a leading question; Doug Tygar was more direct and asked what fraction of goods sold are erotic. Darren replied that FVH does not study the content of the goods it sells, it just collects the money.

In answer to Andy Lowry’s question, Darren suggested that potential sellers of hard goods, such as pizza, are routinely turned away.

Eric Hughes mentioned the potential for Domain Name System hacking to subvert the FVH authorization protocol. Darren conürmed that the potential is there and further that it has been observed in practice, whereupon FVH contacts the responsible authority (*i.e.*, the hostmaster for the domain). This solution may not scale.

Payment Switches for Open Networks
D. Gifford, L. Stewart, A. Payne, and G. W. Treese
Open Market, Inc.

Win Treese described the Open Market system for supporting electronic transactions. A typical transaction involves a Web server with digital offers on it. The customer browses the Web, selects her goods, then presents herself to the payment system to get a digital receipt, which acts as a ticket for goods. The ticket is given to the seller, who conveys the goods.

Open Market supports various payment methods, including credit cards and purchase orders. Authentication can be user-deüned, including challenges such as ‘‘birth date’’ or ‘‘dog’s name.’’ Despite the desire for total anonymity, payment is linked to the good being purchased.

Customer service ordinarily costs several times more than fraud, hence it must be automated. To this end, customers have access to personal, online, up-to-the-minute statements, eliminating the usual monthly statement. Items on the statement contain embedded URLs to more detailed descriptions of transactions.

Because Open Market transactions are inherently nonatomic, good failure semantics are essential. For example, when a customer clicks a button repeatedly, it may or may not mean she wants to purchase several copies of the item.

Answering Hal Varian, Win indicated that Open Market does not yet support discounts based on volume or afüliation. Mark Seiden asked whether receipts are transferable or subject to theft. Win stated that tickets contain IP addresses, among other things, and claimed that tickets are hard to steal, which was met by a general murmur of dissatisfaction.

Jacob Levy observed that in contrast to FVH, Open Market payments take place after goods are delivered. Win noted that FVH itself can be used as a payment system.

John Gilmore complained that he hates shopping, and would like a system that gets him the stuff he needs without his involvement. Win replied that authentication dictates some level of his attention.

1.4. Payment mechanisms

Moderated by Mack Hicks.

Dan Eldridge
DigiCash

Steve Crocker
CyberCash

Dan Eldridge offered some brief remarks. Cash is anonymous and private. Privacy is good. Privacy, once violated, can never be restored. Electronic cash (or coins) is a ‘‘bearer instrument’’ in that the value of the item goes with the bearer. When cash trades hands, the value of the cash immediately belongs to the recipient, in contrast to handing someone a check or performing a credit card transaction, wherein the value goes to the recipient at some unspeciüed future time.

Steve Crocker followed with some remarks of his own. CyberCash is also building payment systems for the Internet. Their goal is to produce component technology to be integrated into other software products. Their software attaches to browsers and servers. The payment mechanism is very similar to other current schemes. They also provide a peer-to-peer payment structure that does not require the transaction-time involvement of banks.

CyberCash uses cryptography heavily; credit card information goes over the net encrypted. Merchants can neither see nor tamper with customer information but are responsible for forwarding it to the bank.

A CyberCash transaction begins when a server makes an offer to the consumer. The consumer sends back credit card information (encrypted). The merchant sends a message to CyberCash to authenticate the customer. CyberCash obtains a credit card transaction from the bank. (Question from the crowd: ‘‘Does it count as a ‘card present’ transaction?’’ Answer: No.) CyberCash sends a ‘‘yes/no’’ message to the merchant, based on authorization from the bank. The merchant sends a receipt to customer.

Steve emphasized the importance of a safe, efücient, and fast mechanism, one that could support small transactions. He stated that there are üve times as many transactions under US$10 than over US$10.

Mack Hicks initiated the panel session by suggesting that payment protocols are less important to banks than whether certiücates such as X.509 or ANSI X.9 are accepted by other banks and payment companies. Steve pointed out that while certiücate standardization codiües the binding between a public key and its certiücation, banks really want to know who you are and whether you will pay your bills.

Richard Field observed that certiücation authorities have a tricky balancing act: they must limit their risk without losing public trust. Mack suggested that certiücation authority may be governmental, reiterating that the process of certiücate acceptance is central.

Andy Lowry agreed with Mack and asked Win about liability if a merchant key is cracked, because this has the potential for enormous losses. Win answered that while keys can be invalidated, perhaps based on checking usage patterns, this does not solve the liability problem. Dan said that liability belongs with the key owner; *e.g.*, if a bank's secret DigiCash key is compromised, the bank is liable for proximate losses. Darren echoed this view, citing recent Utah legislation that places liability with the owner of a digital signature. The crowd responded that 1) this legislation has not yet been tested; and 2) this is a good reason to get out of Utah.

1.5. Payment protocols

Chaired by Clifford Neuman.

NetBill Security and Transaction Protocol

Benjamin Cox, J.D. Tygar, Marvin Sirbu
Carnegie Mellon University

Benjamin Cox described the NetBill protocol, designed for server-based electronic commerce of low-cost electronic items, such as those that would be purchased from a digital library. (The initial deployment sites for NetBill are University digital libraries.) NetBill follows a credit-card model and is optimized for microtransactions and network delivery of goods. NetBill is partnering with VISA and Mellon Bank.

The NetBill protocol is designed so that authorization, payment, and goods transfer are efücient, which will reduce server load, support high volume and availability, and reduce the number of disputes. The goal is for the transaction cost itself to be negligible, to provide for zero-cost goods.

NetBill transactions provide atomicity, non-repudiability, access control, and mutual anonymity and privacy to protect sellers against buyers and buyers against sellers. Transaction atomicity is enforced by a trusted third-party, namely NetBill. Digital signatures are used for non-repudiability. Kerberos tickets are used by customers and merchants for authentication and access control. NetBill runs the Kerberos server.

Tickets have a non-negligible lifetime, which hampers security but improves performance. Public keys are needed for digital signatures, so NetBill extends Kerberos to use public keys for initial authentication. Ben claims this may remove the need for a single, realm-wide Kerberos server.

A NetBill transaction takes place in three phases: price negotiation, goods delivery, and payment. The customer interacts directly with the merchant. A seller can dynamically set the price based on the identity of the buyer, offering discounts based on demographic criteria, such as ''the buyer is a senior citizen,'' *etc.* The customer is also allowed to issue a ''bid'' message to the merchant.

After the merchant and customer agree on a price, the merchant encrypts the goods, sends the encrypted goods to the customer, and waits for payment. The key is sent to the customer upon payment. A copy of the transaction receipt goes to NetBill ï the receipt contains a copy of the key ï in case the merchant refuses to send the key to the customer or if the customer misplaces or fails to receive the key.

Both parties digitally sign the payment receipt, using public key cryptography. Certiücates encrypted by private key replace the Kerberos ticket-granting-ticket. This is just as good as a ticket for identifying the customer, as it uses the public key to authenticate.

In the question period following Ben's talk, Dave Crocker suggested that the credential and authorization mechanisms used in NetBill are a useful generalization and Ben an his colleagues should consider writing an RFC.

In response to Mack Hicks' question about the origin and form of certiücates, Ben stated that NetBill generates the certiücates. Their ünal form depends on the outcome of negotiations with Public Key Partners, Inc. Mack suggested X.509v3.

Mack also asked about liabilities in the NetBill system. Marvin Sirbu replied that an issuer or payment processor must take liability, *i.e.*, NetBill is liable. Doug Tygar elaborated that issues of liability and revocation are clariüed in payment protocols in which transactions run through a trusted server.

iKP ï A Family of Secure Electronic Payment Protocols

M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, M. Waidner
IBM Watson Research Laboratory and IBM Zurich Research Laboratory

Hugo Krawczyk described iKP, a family of secure multiparty payment protocols based on RSA-1024 cryptography. Modeled on the credit card system, iKP has buyers, sellers, issuers, acquirers, and a clearing house. iKP also supports the notion of a gateway, which translates electronic payment requests into clearing house and authorization tasks.

The iKP family consists of 1KP, 2KP, and 3KP. In 1KP, only the gateway possesses a public and private key pair. 2KP provides merchants with keys, 3KP offers full multiparty security by issuing public/private key pairs to customers as well. The choice of protocol is based on the security requirements of the application. In general, the protocol's security guarantee is strengthened by requiring that more parties in the transaction possess and use public key pairs. A family of protocols such as iKP allows for gradual deployment as infrastructure requirements are met.

A Set of Protocols for Micropayments in Distributed Systems

Lei Tang
Graduate School of Industrial Administration
Carnegie Mellon University

Lei Tang believes that Internet electronic commerce trafüc will require micropayments (US$1 or less), and has developed several protocols to support microtransactions. He uses a simple accounting structure and cheap encryption techniques to keep transaction overhead down.

Lei compared the transaction cost of security requirements, symmetric and asymmetric cryptosystems, and payment models. He concluded that security is necessary to keep transaction cost low, that computational intensity and patent licenses make public keys too expensive, and that a debit payment model is simplest. He then presented three protocols that implement these requirements.

Following Lei's talk, Doug Tygar argued that Lei's protocols are neither goods-atomic nor money-atomic, and that a failure could result in an inconsistent state, such as the disappearance of money. Lei responded that modiücations in the protocol could extend them to meet that requirement.

Design Considerations for Lightweight Electronic Payment Mechanisms

Mark Manasse
DEC Systems Research Center

Mark began with some back-of-the-envelope computations. There are 31.5 million seconds in a year, so a computer that costs US$150K per year to run necessitates a revenue stream of one-half a cent per second (assuming constant trafüc). If a ünancial agent skims 2% of the revenue, the éow must be 25 cents per second for the agent to make money. Assuming bursts come in a 10:1 ratio, this requirement is actually US$2.50/second. Assuming the computer can perform 10 encryptions per second, the minimum granularity of a transaction is thus US$0.25.

Improving the granularity of transactions to one cent requires the ability to support 250 transactions per second. To do better than this, say one-tenth cent granularity, requires lumping transactions together, reducing the cost of cryptography, or relaxing some of the guarantees, such as non-refutability, anonymity, or reliability.

Mark then presented Millicent, which uses scrip to support ''femtopayments'': very lightweight transactions whose costs are fractions of pennies. Millicent is designed for transactions such as a payment per Web access, per stock quote, or per index query. Millicent sacriüces anonymity and non-repudiation to accomplish its ends.

Millicent is a broker that issues unforgeable scrip in large amounts, say US$5, but broken down into small units, each with a unique identiüer. Scrip is issued for use with a speciüc merchant. The merchant veriües that the customer spends each identiüer no more than once. Scrip that expires can be refreshed by the broker.

The question and answer period for Mark's talk was lively as participants tried to grasp the details of Mark's system and compare the four systems discussed. Jill Ellsworth asked Mark if concern about government regulation is important in micropayment systems. Mark responded that he has no deünite information on the government's interest in micropayments. There was a éurry of responses (most from Marvin Sirbu) that the government is worried about the broad use of encryption, but not its narrow application to electronic commerce. The current status is that the transfer of bulk encrypted documents is legal, but the export of encryption technology is not.

Win Treese wanted to know how a 5% sales tax would be handled on a 1/100th cent purchase. The consensus was to round down.

Doug Tygar suggested that it is difücult to differentiate between so many protocols in one session, especially ones that seem to occupy very different regions of Jean Camp's taxonomy. Cliff Neuman felt that we will have to wait and see how the various systems behave in large volume. Doug added that even though STT appears inappropriate for microtransactions, it should also be considered, because with it, VISA and Microsoft will control a large chunk of the market.

Robert Gezelter asked how a merchant can tell whether scrip is legitimate and how payment authorization is accomplished. Mark responded that the scrip is merchant-speciüc and that transactions are pre-authorized. Robert questioned whether current laws permit issuance of private scrip. Richard Fields suggested that it is allowed.

1.6. Dinner speaker

Marty Tenenbaum
Enterprise Integration Technologies

Marty Tenenbaum opened his after-dinner address with the observation: ''It's been a hell of a year for the Internet ... and you ain't seen nuthin' yet!'' A year ago, when CommerceNet started, people said Internet commerce was either illegal or immoral. Now, according to the Economist, it's bigger than the telephone and approaches the printing press in its impact to society. The Web has unleashed the Internet marketplace, and with the new inéux of security into the Web, we'll really see commerce sprout.

CommerceNet was born in February, 1993 at the Sheraton New York (coincidentally, the workshop meeting place), during a meeting of the Technology Reinvestment Program. It is a consortium of over 120 American companies, such as Citibank, IBM, MCI, Netscape, UC Berkeley, and Wells Fargo. CommerceNet is growing at the rate of about 10 new companies per month, with basically no marketing. A CommerceNet Japan chapter is also starting. CommerceNet has working groups exploring, developing, and exploiting emerging technologies. Most of the action takes place in these working groups.

CommerceNet provides a brokering function by disseminating multimedia catalogs; hypermedia browser starter kits (a service no longer felt to be necessary); ISDN connectivity and networking hardware and software; specialized directories, *i.e.*, those not obviated by Yahoo and Lycos and their ilk; security (encryption and authentication); and payment services (credit cards, debit cards, checks). All this works to support collaborative engineering products.

CommerceNet hopes to replace EDI, which requires prior arrangements between trading partners, with Internet storefronts based on Web browsers. Marty described PartNet, a place where parts are available, and the Internet Shopping Network, which replaces rooms full of ''operators standing by'' with Web servers.

The impact of electronic commerce in the short term will be to cut costs, shrink development cycles, and streamline procurement. The long-term outlook is the atomization, or disintegration, of vertical companies into ones offering core competencies in niche areas, outsourcing the rest. This will empower small businesses, niche publishing, and tiny markets and will lead to new information services, such as risk management and brokers to bring buyers and sellers together.

2. Wednesday, July 13, 1995

2.1. Technology

Moderated by Peter Honeyman.

Smart Catalogs and Virtual Catalogs
Arthur M. Keller
Stanford University

Arthur Keller opened by asserting that just as important as transaction security and payment for goods is the ability to *locate* things on the net.

Current online catalogs use the Web, in which documents are typically menus pointing to other documents. Each vendor maintains its own menus, an approach that has limitations: it's hard to ünd what you want when the menus are organized by company as opposed to by product For example, it is not possible to query `www.printers.com` for cross-listing of references to every commercially available printer. Furthermore, there are no standards for organizing information, so each catalog has its own unique structure. In addition, there is often no facility for searching by content and no support for cross-catalog searching.

Some of the queries we might want to issue include: ''Give me list of local dealers for the HP DeskJet 1200C PostScript printer''; ''Give me a list of all HP printers for the Macintosh''; ''Notify me whenever someone announces a color PostScript printer for the Macintosh less than $3000''; or ''Give me a list of *any* merchant's color PS printer under $3000.''

Support for these types of transactions requires distributed searches; support for ''reverse'' or content-based search, *e.g.*, to look for printers or disk drives, not product names; support for heterogeneous information sources; getting the information from the horse's mouth, *e.g.*, get information on Hewlett-Packard printers from HP, not from someone else; and cross-searching of multiple catalogs.

The CommerceNet Smart Catalog project supports all of these requirements. The system is composed of distributed agents that speak a common language and translate between it and the individual languages of the merchant catalogs (such as SQL, *etc*.).

The system also allows distributors to make ''virtual catalogs'' based on smart catalogs. By pointing its virtual catalog at the smart catalogs of its manufacturers, a distributor can provide a consistent interface to its customers. The interface can also be more complete, as it avoids handing off control to the manufacturer, which presents a problem if information must be transferred back to the distributor's catalog service.

CommerceNet queries to manufacturers result in information in forms like product description = <text>; product picture = <gif>; product specs = <text>; *etc.* An intermediate browser, virtual catalog, or CAD tool can do with the information as it pleases, allowing distributors to customize and personalize their Web page layouts and organizations.

The system also contains Facilitators, or intermediary agents along the lines of X.500 directory agents, responsible for keeping pointers about speciüc product types, such as TOASTERS or PRINTERS or FOOD. Finally, Smart Catalogs support Ontologies. There must be standard languages/grammars for each product type available via the system. Standards organizations will deüne the highest-level languages, and every database must use the deüned names for item labels. Lower-level languages, as needed per speciüc product, can be deüned by the manufacturer of the product.

Robert Simoncic asked whether CommerceNet offers a new way to get into price wars. The distributor does not need to stock the product, so what stops each manufacturer from bidding down at transaction time? Arthur speculated that new business and commerce models will appear for precisely this reason.

Alan Nemeth pointed out that caching the results to queries may be a problem if these results don't remain valid for too long. Arthur agreed that this is important and will be looked at when virtual catalogs are built.

Robert Gezelter asked about bottlenecks and system overload. Arthur joked when you know an important bid is coming, you could swamp your competitor's catalogs with queries. In seriousness, he advised that it is possible to put a ülter on the system, or send information out only to accepted endpoints, but this is also future work.

Safe Tcl: A Toolbox for Constructing Electronic Markets
Jacob Levy and John Ousterhout
Sun Microsystems Laboratories

Jacob Levy spoke about electronic meeting places and using Safe Tcl to build them. Electronic meeting places are virtual spaces where mobile agents (represented by code+state) can run. The spaces have persistent state and provide a consistent view to all of the mobile agents currently in a room. Possible uses include advertising and commerce, social interactions, integrated currency, advertising methods, ordering and delivery of goods, *etc.*

Safe Tcl offers a way to run these electronic meeting places. Safe Tcl handles multiple address spaces within a single process by running a different Tcl interpreter in each address space. This allows execution of code that is not trusted or of communicating scripts that do not trust one another. System calls and IPC requests are processed by intermediary agents that allow actions based upon authentication.

A Safe Tcl environment has a hierarchical structure in which parent threads create children threads. Each thread is a separate Tcl interpreter.

An interpreter's execution restrictions are set by its parent. Children must trust the parents, but the parents do not trust the children.

Safety is provided by ensuring that only known good code is run by unrestricted interpreters. Untrusted code is run by restricted interpreters.

In Safe Tcl's underlying trust structure, trust is not based on *where* code is from, it relies on *who* code is from, authenticated using digital signatures.

Multiple interpreters with different restrictions isolate concurrent executing scripts. Removing functionality makes them safe from each other.

Open problems in safe execution include protecting a mobile application (a script that moves between meeting places) from the hosts, persistent scripts, and the absence of standards.

Ben Cox asked about combining safe elements in unsafe ways, for instance, a pop-up box that asks for the user's credit card number and then relays the information to someone else. Jacob replied that the problem of user gullibility is something that he plans to address.

Arthur Keller asked how Safe Tcl decides what scripts run on which interpreter. For example, you don't want a privileged interpreter to be able to grant person A üle access to a script written by person B. Jacob responded that scripts are authenticated as if they are the actual person; a script cannot do things that the person cannot.

Developing and Deploying a Corporate-Wide Digital Signature Capability
Diane E. Coe and Frank J. Smith
The MITRE Corporation

Diane Coe described current cryptographic efforts at MITRE, which include digital signatures, a key management system, distributed authentication, and a system integrating these various aspects. MITRE's interest in digital signatures stems from a belief that they can help lead to the paperless ofüce and thus save time and money.

MITRE's efforts are based on the RSA BSAFE toolkit, using RSA for authentication and MD5 for hashing. SIGN and VERIFY functions are part of a software package that is easily embedded into other applications.

MITRE uses a key management system integrated with the X.500 directory structure for authentication. Users go to a key generator for a key. The generator places the key and a certiücate onto a éoppy disk or smartcard. The certiücate is also stored in a certiücate database and in the user's X.500 entry.

MITRE uses Kerberos-based distributed authentication. This provides single sign-on capability using Kerberos credentials and passwords for proprietary and residual systems. They are moving from éoppy disk to smartcards for security reasons.

MITRE has run into horrible interoperability problems: only rarely can credentials be shared between different systems. Most products are not open and the ISO smartcard standard is still evolving, so interoperable products are only just emerging.

MITRE's Kerberos realm ends at the edge of MITRE. To communicate with the rest of the world, MITRE has followed the relevant standards: X.500, X.509, Kerberos, RSA, *etc*., but there is not yet any advantage to having done so. Credit card companies are building their own systems and digital signature capabilities; MITRE fears it will need a different smartcard for each bank. ''Everyone says they're singing from the same sheet of music, but they're not singing the same song.''

Marvin Sirbu asked whether the fact that a token contains only one key-certiücate pair means that you need a smartcard for every certiücate authority. Diane responded that this depends, *e.g.*, on whether VISA uses your key or issues their own. Marvin suggested that if you can set up the token so it can hold multiple certiücate-key pairs, then you solve the problem. Greg Rose suggested that you get a certiücate-key pair out of each token and put them into a universal one.

Greg asked Diane why MITRE didn't go to a hierarchical system instead of one certiücate authority. The answer was simple: Cost.

In response to Juan Rodriguez' question, Diane conürmed that the date on the éoppy signature is protected by user password encryption.

Answering Arthur Keller, Diane said it is impossible to masquerade as someone if you ünd their éoppy or smartcard, as you also need their PIN/password to unlock the smartcard.

John Gilmore wondered why MITRE chose the ISO smartcard over PCMCIA, as the latter offers access to many more readers. Diane responded that the smartcards üt into MITRE's existing badge readers.

Bob Gezelter asked whether the credentials in the smartcard go over the network. Diane agreed that would be a huge security hole, and stated that the credentials are read by the card reader but go no further than that in the clear.

2.2. Extensions

Chaired by Marc Donner.

Digital Notary
Stuart Haber
Bellcore

Stuart Haber described Surety Technologies, a commercial spin-off from Bellcore whose initial product is a digital notary, used to prove that a given document existed in a certain form on a certain date. A sample use is notarized electronic lab notebooks to defend a patent.

Stuart provided a concise overview of the operation of the notary. Customers convey digital documents to Surety. Periodically, Surety constructs a binary tree, with the MD5 hash of each document stored at the leaves. The interior nodes are also labeled with hash values constructed from the combined values of the node's immediate children. The value of the node at the root of the tree is published (in the Sunday New York Times). Each customer is then given the hash value of her leaf document, as well as the hash values of all nodes adjacent to the nodes on the path from root to (customer) leaf. With these hash values in hand, the customer can prove that her document contributed to the published hash value.

The hash function is one-way, so possession of a collection of values that produce the published hash value is ürm evidence that the customer's document existed prior to the publication date. Furthermore, because the hash values are constructed in a tree, the number of values returned to the customer is equal to the height of the tree, so the procedure scales with the log of the number of documents. Additional scaling can be had by allowing local servers to build their own trees, transmitting the root hash value to a Surety tree. The system has no keys to compromise and appears to be extremely secure.

In answer to Richard Field, Stuart reiterated that Surety need not retain copies of the documents or even the intermediate or root hash values. The customer is given all the tools and values necessary to recompute the root hash value.

Generic Extensions of WWW Browsers
Ralf Hauser and Michael Steiner
IBM Zurich Research Laboratory

Ralf Hauser described the need for a ''snap-in'' product to put into Web browsers that offers security and payment methods. He found that this is not really possible: you need to modify servers or add processes to systems. Ralf went on to describe a better way to architect Web browsers, but the audience resisted the notion of changing everyone's browser or even considering more work in this area when Java and Safe-Tcl are just now appearing.

The initial goals of generic extensions to WWW were to support iKP security without modifying browsers. Current needs include security when making purchases. Several possible architectures were described. One relies on MIME to invoke a local payment client, which contacts a payment server to complete the actual purchase. This does not easily admit post-processing. Another architecture uses a proxy Web server that intercepts and processes payment requests; ürewalls can make this quite challenging.

Ralf argued in favor of a generalized architecture, which includes an extensions manager, passive extensions such as ülter viewers, and active extensions such as remote controllers. The extension manager handles not only MIME, but also HTML as an HTML-viewer extension.

John Gilmore asked how to accomplish these ends in a way that is not speciüc to any particular browser. Ralf answered that while binary compatibility is required, it's as generic as MIME. Rohit Khare elaborated by comparing to CGI, which differs among the various platforms. But John would not be satisüed with anything less than Java or Tcl.

Rohit asked about versioning for the client-side, to make sure the latest version of security is being used. Ralf suggested placing the version number in the MIME type, as the architecture is transparent to that issue.

Andy Lowry observed that the generic extensions approach doesn't push in a direction for patching together distributed applications, especially long-lived ones and gave the IBM SOM product as an example. Ralf felt that because HTTP is stateless, SOM could be supported under the architecture.

Andy followed up by suggesting the importance of long-lived processes internal to an organization. Ralf responded that the work described here is in the vein of a browser and renderer; long-lived processes can be launched from the browser, but anything more is beyond its purview.

Secure Coprocessors in Electronic Commerce Applications
Bennett Yee and J.D. Tygar
Carnegie Mellon University

Bennett Yee characterized the fundamental problem of electronic commerce as the distribution of security and argued that hardware should play a role. Secure coprocessors are capable of solving some of the problems that software solutions can't.

A secure coprocessor is a standard microchip and some NVRAM in tamper-proof packaging. Potential form factors include chips (such as the infamous Clipper/Capstone), smartcards, or PCMCIA. Bennett maintains that technology for physically secure hardware is a reality.

A secure coprocessor is a safe place to store cryptographic keys as well as to do some computation. In one application, a secure coprocessor can be used to ﬁght software piracy by enabling delivery of encrypted software. The secure coprocessor holds the crypt key and runs the decrypted code. Everything sent to the host machine, including paged data, is encrypted before it goes out. This scheme protects applications, but not data. For example, a protected picture must be decrypted to view it, at which point the protection may be lost.

A secure coprocessor provides a very simple scheme for electronic money: the coprocessor knows how much money it has allocated to it, and tampering results in loss of cash. Such a system can be much safer than DigiCash, where it is possible for a merchant to not receive the packets necessary to reconstruct the money (and here, Bennett gave an extremely effective demonstration of the fragmentation of digital money over the net by ripping up a dollar belonging to Ben Cox), or to pretend that it never got the packets. Using secure coprocessors, neither side of a transaction can be tampered with and protocols can be run as transactions, with ACID properties guaranteeing that money is either transferred completely or not at all.

Point-of-sale is another potential application, using a secure coprocessor as a debit card. To protect against Trojan-horse merchant systems, the coprocessor should allow the customer to enter a password to approve the withdrawal of funds and to verify the amount. Bennett described a simple method for ensuring that the merchant system does not get the password: the coprocessor displays a random string and the customer uses arrow keys on merchant's system to change the values to the correct password.

A secure coprocessor also allows transmission of sensitive materials to other processors using public key encryption. Such a scenario appears to be impossible with Safe Tcl or Java.

Mack Hicks asked whether secure coprocessors can offer virus protection. Bennett answered in the afﬁrmative, and outlined one scheme.

John Gilmore asked how to protect users from malicious cards that do not allow them to ''read the code.'' There seems to be no satisfactory answer, but Bennett favors openness.

Eric Hughes delved into atomicity issues in communications between coprocessors over unreliable networks; Bennett referred him to the literature on two-phase commit protocols.

The DigiBox: A Self-Protecting Container for Electronic Commerce
O. Sibert, D. Bernstein, and D. Van Wie
Electronic Publishing Resources

Olin Sibert argued that one of the requirements of electronic commerce is a container mechanism that protects itself as well as its contents from tampering. For example, currently an author writes a book, or an artist composes music, *etc.* When it comes to being reimbursed for the actual number of copies produced and sold, the creator of the work is at the mercy of the publisher, with no way to ensure that the number of copies the publisher claims is the number of copies actually out there. This is compounded by consumers making their own copies of the work, cheating the copyright system. How can the rights of the creator be protected?

One of the main disincentives for breaking copyrights is purely physical: the price of a book is generally lower than the hassle to sit at a copier for the many hours it takes to make the copy. The computer and digital information technologies open up new ways to be exploited, but also open up new ways to protect copyrights.

Olin described DigiBox, a generalized container that holds and protects arbitrary information content. Users pay for the keys before the container will hand over contents. Containers can hold many different items, *e.g.*, several books, movies, audio recordings, and divulge only one part at a time.

A complex key management system allows portions of the keys to be divulged, with items in the container being encrypted by several different key fragments.

Olin's scheme uses selective encryption for performance reasons: encrypting a small fraction of an MPEG üle makes it just as useless as one that is fully 100% encrypted. For audio, the entire üle is encrypted, but the key changes periodically. Each key can be less secure (for faster implementation) but the net effect is no loss of security.

DigiBox has many applications, such as discount coupons, key escrow, arbitrary content, *etc.*

Noting that the key mechanism is extremely complex, Marc Donner asked what sort of attacks it is meant to defend against. Olin responded that DigiBox allows multiple copies of a mass-produced product to have different keys for opening it. Part of the complexity is to ensure that one divulged key can not open every copy of a container.

John Gilmore cautioned that software and keys don't mix very well in the real world. Olin suggested that an approach that combined DigiBox and secure coprocessors might offer more stringent security.

Kerberos Plus RSA for World Wide Web Security
Don Davis
Consultant

Don Davis, veteran security guru from the Kerberos project, described his displeasure with other Web security systems and suggested an approach that combines strange bed-fellows Kerberos and RSA with minor protocol enhancements. Don's gripe with SSL is that it doesn't authenticate servers, just clients, which may leave consumers vulnerable to credit card fraud. SHTTP, on the other hand, makes too many homogeneity assumptions, forcing both sides to use either public keys or Kerberos.

Don's scheme requires some changes to the Kerberos protocols. Touted advantages include obviating the necessity of a key database (thus diskless operation) and improved revocation. The scheme seems to have many administrative and performance advantages.

In an interesting side-comment, Don recently discovered and documented an oversight in the Kerberos protocols: it turns out that Kerberos client clocks don't need to be synchronized.

Bennett Yee asked about Trojan horse attacks in distributing patches; the crowd responded ''CERT.'' Don pointed out that distributing patches is an iffy way at best to correct existing ills, as there is no certainty that vulnerable sites will install patches, in fact bitter experience proves otherwise.

2.3. Luncheon speaker

Alliance Ecology: A Key to Strategic Success in Electronic Commerce
Bud Mathiasel
Ernst & Young

Bud Mathiasel, Director of Multimedia Consulting Services for Ernst & Young, opened by asking the audience who will beneüt from a global multimedia market? The answers included Microsoft, Sony, Netscape, Disney, SGI, AT&T ï all the usual suspects. Bud maintains that no one will do it alone, and offered many examples of the alliances being formed among information technology players, as everyone realizes the risks in going it alone.

As bandwidth grows, so does the complexity of its use as applications take advantage of its potential. Bud identiüed a general trend, which he called ''disintermediation'' ï the removal of intermediary points between context, content, and infrastructure. (This is similar to Marty Tenenbaum's notion of dis-integration of vertically integrated manufacturers.) As an example, Bud observed that automated teller machines eliminate tellers, giving customers a more direct association with their banks.

Other trends are the movement from marketplace to ''marketspace'' and from ''clockware'' to ''swarmware.'' Peter Honeyman to Andrew Hume: ''Kill me now.''

In general, Bud's comments left folks reeling. There were many polite, but confused, questions. Jacob Levy was heard to observe, ''What he's saying is that we want a kinder, gentler marketplace.''

2.4. Electronic commerce in the real world

Moderated by Win Treese.

Darrell Davis
Lombard Technology Group

Andy Lowry
Morgan Stanley

Howard Alt
Sun Microsystems

Andy Lowry began by describing Morgan

Stanley, which carries out extremely high-value transactions for a small client base in a highly regulated market. Morgan Stanley uses the Internet for commerce, in part because of ‘‘a critical mass of clients and business partners there’’ and is now exploring the use of the Web as a generic service delivery platform already in place with a clean split between client and server. Using the Web is also good for corporate public relations.

The big question, naturally, is security. Authentication and authorization are absolutely critical. If unauthorized people back out on large transactions, Morgan Stanley is stuck with the costs. The solutions being employed include key escrow, trust management, and risk management.

Open questions abound, such as the liabilities when a trade is based on a certiücate whose key has been compromised, or how to place performance guarantees (time of delivery, or even delivery at all) on the net. For example, if someone submits a TRADE message just before the close of the market, and the delivery of the message happens *after* the close, who is responsible? Answering his own question, Andy suggested that insurance, classic risk management, will play a role.

Next, Darrell Davis described some of the challenges faced by Lombard Technology Group, which will soon be selling stocks and other instruments through the Web. Lombard uses the Netscape commerce server through a ürewall to provide portfolio management for its clients.

Some of the challenges faced when a naive management decides to go mission-critical with a new and popular service include a boss who is gung-ho about performance but not about security; neglecting customer support in initial plans, requiring developers to be pulled off other work; providers that don’t support SSL or even Web browsers; and exponential growth in trafüc.

Howard Alt spoke next, explaining that Sun sees a different picture of the world. Sales do not go to the customer: they go through channels. The sales channel creates demand and enables volume. When you bypass your channels, you aggravate them. It is a bad thing to aggravate sales channels.

Sun regards the Internet as a means of delivery, not a channel, and wants their electronic agreements to include sales channels. He also pointed out that while Sun wants copy protection, key-based service denial is not their goal. (It is a problem when a customer has bought a software package but cannot run it because the license server is down.)

Black-box technology is bad: magic secrets are not reasonable in the real world. It is hard to control too many secrets. In contrast, the cryptography people got it right: the algorithms are public knowledge, the implementations are public knowledge, only the key is secret. Limiting the number of mysteries is a worthwhile goal.

In the panel discussion, Darrell reported that Lombard receives about 100,000 HTTP requests per day, about a third of them for stock quotes, and the rest for graphs. 400 requests per day for new account information is typical, and about a quarter of these result in new customers. Lombard’s server generates graphs dynamically with Gnuplot, which is killing the system, as is a horribly slow RAID 5 system. Other than that, the server has sufücient capacity.

Darrell would like to have better tools for authentication. Lombard uses account number and password, similar to other trading companies, and not challenge-response because it is hard enough to get clients to plug in their modems and use the right browser.

Rohit Khare asked why we are content with weak security on the phone and yet we expect so much from the Internet. Bob Gezelter replied that it is easy to tap into the net and overhear thousands of circuits, but tapping a phone line taps only one circuit.

Andy observed that we’re going to have a very rich set of certiücates in the future. Howard noted that while the Web is great for retrieving information, it lacks management tools and standards necessary for commerce. Mark Seiden suggested that stable URLs are a valuable asset, just like a stable 800 number.

2.5. Breakout sessions

In the breakout session, the workshop broke into small discussion groups to address issues of liability, offshore jurisdictions, privacy vs. anonymity, and intermediate success and failure in economic commerce. The workshop then reconvened to discuss these issues in the larger forum. A panel with one representative from each group was formed by Ittai Hershman, Jacob Levy, Peter Honeyman, Dan Geer, and Eric Hughes.

Who is liable?

Eric Hughes' answer was simple: someone else. Ittai Hershman suggested that laws have always been slow to adapt to new technologies; we need to think in terms of the credit card paradigm (which includes a customer, a merchant, and a bank). As far as liability, people will sue the person they think *can* and *will* pay. Joe Arceneaux offered a comparison to hazardous goods, where a broad spectrum of risk-allocation methods are already in place.

Dan Geer offered a new perspective: the person who needs to believe is liable. If I need to trust a fact and it turns out false, I am liable. If the fact is backed by a guarantee, and the guarantor needs to believe something else (like the customer will pay, or the customer has been authenticated), the guarantor is liable. Ben Cox noted the similarity to PGP's “web of trust.”

Lee Parks suggested that this is similar to a consumer's responsibility to protect her credit card and PIN number; it is her obligation to report the theft of her card immediately. Lee offered a question from the hard-boiled school: When bad things happen, who will the legal system point the ünger at?

Richard Field held that the belief argument is circular: you're liable because you need to believe, and you need to believe because you are liable. Ittai Hershman observed that courts are likely go with precedence rather than shift to new, untested rulings. Eric Hughes made a comparison to warrants in existing systems: a check implies the existence of funds in your account.

Peter Honeyman argued that liability is built into the price of the transaction based on a market for risk acceptance and management.

Privacy is a right; anonymity is a shield for criminals.

Ittai Hershman pointed out that different levels of anonymity exist. When you go down to the corner video store and rent a porno video you have *virtual* anonymity in the implicit assumption that the clerk will not reveal your name even if he recognizes you. If you purchase your own copy for $20 in Times Square, you have *real* anonymity. Ittai suggested that society will not tolerate *real* anonymity on the Internet.

Jacob Levy claimed that privacy is a commodity, for sale like any other. There was widespread disagreement with this position. Andrew Hume argued, “That's a bald-faced lie. You can't buy privacy *today*.” There was general dissent to this, as well. Greg Rose suggested that if you can buy privacy, someone else can buy a breach of it.

Joe Arceneaux argued that even if anonymity IS a shield for criminals, it has its uses and good points. Privacy is a policy issue; anonymity is a technology issue. Dan Geer pointed out that anonymity is not binary, *i.e.,* it's not the case that you either have it or you don't. Rather, one has privacy within a certain domain. For example, it is desirable to distinguish between one's private and commercial lives: it is not advantageous to offer someone anonymity while on the job if the company is liable for the worker's actions. Furthermore, while anonymity is the only shield against data aggregation, the law will inevitably require *some* breach of it.

Peter Honeyman offered the view that the central question is one of social control. For example, Swiss bank accounts pay less interest on anonymous accounts. Privacy seems to have less value today than it has had in the past.

Eric Hughes offered four maxims: anonymous systems are hard to audit and adjudicate; anonymity decreases as the transaction size increases; “when cash is suspect, only suspects will have cash”; and liquidity substitutes for identity.

Dan Geer offered an alternative viewpoint: anonymity is the best shield *against* criminals. Josh Rabinowitz agreed that anonymity protects “normal” people.

Andrew Hume maintained that privacy is all the average person *really* wants. Anonymity is nothing more than an implementation issue.

Eric Hughes gave two examples. Chaum's DigiCash provides anonymity to the common man. On the other hand, Morgan Stanley has run full-page ads offering anonymity (actually, pseudonymity) for large ünancial transactions.

Ben Cox suggested that changing a pseudonym often enough effects anonymity, but this provoked widespread dissent. Eric Hughes pointed out that only the ürst use of a pseudonym is truly anonymous. Peter Honeyman noted with some sarcasm that “those who have nothing to fear have nothing to hide.” Dan Geer held that electronic commerce promotes data aggregation and that anonymity is the only protection.

Andy Lowry asked whether we should be doing something about these issues besides talking about them, such as forming a CommerceNet working group.

What will move offshore?

Joe Arceneaux proposed that in the short term, socially disapproved industries such as pornography and gambling make the transition to offshore operation. A long term is less sure. The big question is privacy: if going offshore increases the level of privacy, it is an enormous advantage. However, many activities will remain traceable, and it will be harder and less desirable to set up your own business offshore. Dan Geer pointed out that today's networks already make things location-independent. The question is what would keep a business *onshore*?

One possibility is the protection of the legal system, which suggests that you would choose a physical location for its legal codes. Electronic services will likely move offshore because there is no disadvantage, such as shipping costs. Industries that respond to bids, like artwork, copy writing, programming, *etc*., will easily be placed offshore. Also, support operations are likely to make the transition because of reduced costs; for example, today, many 800 number support lines go to places in the Midwest for economic reasons. When you call an airline, or the mail order catalog, the person answering the phone is usually *not* located in the corporate headquarters because of *cost.* These types of operations will go wherever it is most cost-effective.

Peter Honeyman suggested that operations will move offshore because it is economical or required to do so. When people see that the Lithuanian Web server is generally underloaded, there will be a rush to move there. Peter questioned the efficacy of moving out of a jurisdiction, raising the example of the California erotic BBS convicted of violating Memphis community standards.

Eric Hughes replied that Internet carriers are enhanced services providers, *not* common carriers, so that different laws apply to them. Amplifying Eric's comment, Hal Varian noted that a common carrier is protected from liability for the contents of what is carried, while enhanced services providers *are* liable for the contents. Arthur Keller pointed out that the question of common carrier status can be murky, *e.g.*, cable TV providers are liable for the contents of their transmissions.

There was a general feeling that much software development will move offshore, enabled by the Internet. Peter noted that the University of Michigan Digital Library project has its digital scanning done in Barbados.

Eric suggested that while moving offshore has anonymity and regulatory advantages, these are offset in part by a disadvantage in restrictions on import/export.

Who dominates electronic commerce in the year 2000?

There was general agreement that the entertainment industry will be a big winner.

In Dan Geer's breakout group, the primary question was what the infrastructure will look like. Dan restated the question by asking whether the dominant players will be new, unforeseen businesses enabled by electronic commerce or whether they will be revamped, old businesses. Will service providers like AOL, Compuserve, and Prodigy still be around? Will there be a global provider or regional carriers? Another fundamental dichotomy: Which wins more, content or context, *i.e.*, the stuff or the transport?

Peter Honeyman suggested a different dichotomy: Spielberg vs. CU-See-Me (extended to CU-See-Me-CU, *etc*.), *i.e.*, the little guy or the big guy? Clearly, VISA, Mastercard, AMEX will win; all schemes presented involved the credit card companies in one way or another. Peter's one-word summary: turmoil.

Joe Arceneaux agreed that credit card companies will win, as well as other transmogrifications of present financial systems, enabled by the new commerce paradigm.

Jacob Levy offered the view that one big winner is the customer, who will have a much wider selection of choices than ever before. Winners will include the providers of funding, hardware, and information. Losers will include banks that do not adapt and the poor, who will suffer lack of access. This was met by some disagreement over whether the rich and the poor will have such a great degree of disparity in access to electronic services. Jacob asked how many poor people have bank cards. Someone in the crowd asked how many have cars.

Peter suggested that the decreasing cost of technology has a democratizing force. Joe Arceneaux said that when Al Gore spoke in South America about the Internet as a force to bring democracy to them, his audience was less than enthusiastic, as they seem to hold a dim view of American democracy. Richard Field pointed out that third world countries that have missed out in the last few generations of technology can leap-frog cheaply and easily into the global mainstream. Andrew Hume pointed out that in surprisingly aféuent places, you still see people who cannot afford even modest monthly connect fees. Peter argued that we're moving the cost line down. Andrew replied that we're moving the poverty line up. Andrew went on to say that when Bell Labs tried to offer free access to public libraries by donating machines, the libraries couldn't afford the cost of continuous access.

Eric Hughes suggested that nobody will dominate, just as no one ''dominates'' today. Obvious winners include the credit card systems. Obvious losers will include paper mail-order businesses, salespeople and securities traders who lose their jobs, and technical people like Web administrators will lose quality of life.

Andrew Hume argued that the mail-order industry is making *so much money* that electronic commerce would need to *completely* swamp the market to hurt them. You won't hurt L.L. Bean for a *long* time. It was pointed out that L.L. Bean is on the net already.

Ittai Hershman stated that capitalism will be a big winner.

Richard Field felt that the federal government will deünitely win.

2.6. Wrap-up

Daniel E. Geer, Jr. Sc.D.
Open Market, Inc.

After an enthusiastic show of interest in holding another workshop in the near future, Dan Geer offered some closing remarks and adjourned the workshop.

Acknowledgements

This digest was produced with the assistance of student scribes, Sarah E. Granger, Bruce Jacob, Trent Jaeger, and Charles Thayer, who diligently recorded the presentations and followup discussions; their efforts are warmly appreciated. Scott George lent his quick and careful eye to a draft of this digest. The workshop itself was the brainchild of Daniel E. Geer, Jr., Sc.D., who accomplished the impossible by taking it from conception to fruition in six and one half months.