Electronic Banking and Information Assurance Issues: Survey and Synthesis

Manish Gupta, Raghav Rao, Shambhu Upadhyaya
State University of New York, USA

ABSTRACT

Information assurance is a key component in e-banking services. This article investigates the information assurance issues and tenets of e-banking security that would be needed for design, development and assessment of an adequate electronic security infrastructure. The technology terminology and frameworks presented in the article are with the view to equip the reader with a glimpse of the state-of-art technologies that may help towards learned and better decisions regarding electronic security.

Keywords: e-banking; information assurance; Internet banking; Internet security; issues, services and mechanisms.

INTRODUCTION

The Internet has emerged as the dominant medium in enabling banking transactions. Adoption of e-banking has witnessed an unprecedented increase over the last few years. Twenty percent of Internet users now access online banking services, a total that will reach 33% by 2006, according to the Online Banking Report. By 2010, over 55 million U.S. households will use online banking and e-payments services, which are tipped as “growth areas”. The popularity of online banking is projected to grow from 22 million households in 2002 to 34 million in 2005, according to Financial Insite, publisher of the Online Banking Report newsletter.

Electronic banking uses computer and electronic technology as a substitute for checks and other paper transactions. E-banking is initiated through devices such as cards or codes to gain access to an account. Many financial institutions use an Automated Teller Machine (ATM) card and a Personal Identification Number (PIN) for this purpose. Others use home banking, which involves installing a thick client on a home PC and using a secure dial-up network to access account information, and still others allow banking via the Internet.

This article will discuss the information assurance issues (Maconachy, Schou & Ragsdale, 2002) that are associated with e-banking infrastructure. We hope that the article will allow Information Technology managers to understand information assurance issues in e-banking in a holistic manner, and help them make recommendations and actions to ensure security of e-banking components.
INTERNET/WEB BANKING

A customer links to the Internet from his or her PC. The Internet connection is made through a public Web server. When the customer brings up the desired bank's Web page, he or she goes through the front-end interface to the bank's Web server, which in turn interfaces with the legacy systems to pull data out for the customer's request. Pulling legacy data is the most difficult part of Web banking. While connection to a Direct Dial Access (DDA) system is fairly straightforward, doing wire transfer transactions or loan applications requires much more sophisticated functionality. A separate e-mail server may be used for customer service requests and other e-mail correspondence. There are also other middleware products that provide security to ensure that the customer's account information is secured, as well as products that convert information into an HTML format. In addition, many of the Internet banking vendors provide consulting services to assist the banks with Web site design and overall architecture. Some systems store financial information and records on client PCs, but use the Internet connections to transmit information from the bank to the customer's PC. For example, the Internet version of Intuit's BankNOW runs offline at the client and connects to the bank via the Internet only to transmit account and transaction information (Walsh, 1999).

In this section, we discuss some of the key nodal points in Internet banking. These points are the foundations and principal aspects of e-banking: Web site and service hosting, possibly through providers; application software that includes middleware; regulations surrounding e-banking and standards that allow different organizations and platforms to communicate over the Internet.

Web Site & Banking Service Hosting

Banks have the option of hosting Web sites in-house or outsourcing to either service bureaus or core processing vendors with expertise in Internet banking. Whether outsourced or packaged, Internet banking architectures generally consist of the following components: Web servers; transaction servers; application servers; data storage and access servers. Vendors such as Online Resources offer a package of Web banking services that include the design and hosting of a financial institution's Web site and the implementation of a transactional Web site. Online's connection makes use of the bank's underlying ATM network for transactions and real-time bill payment. In addition, optional modules are generally available for bill payment, bill presentment, brokerage, loan application/approval, small business, and credit cards. The fact that multiple options of Web hosting exist also brings with them issues in security and privacy - a topic that is considered in a later section.

The components that form a typical Internet banking initiative are shown in Figure 1.

- Internet Banking Front-End: The front-end is often the client-side browser access to the bank's Web server. Client-side thin-client access to the bank's Web server: This model allows the customer to download a thin-client software product from the bank's Web site and may allow storing financial data locally. Client-side thick-client access to the bank's Web server: This is the model used when supporting personal financial management packages as tools to access account data and execute transactions. It is important to note that these models are not mutually exclusive of

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Internet Banking Transaction Platforms: The Internet banking transaction platform is the technology component that supports transactional processes and interfaces between the front-end user interface and the back-end core processors for functions like account information retrieval, account update, and so forth. In general, the transactional platform defines two main things: (1) the functional capabilities of the Internet banking offering (e.g., whether it offers bill payment or credit card access) and (2) the method of access or interface between the front-end and back-end legacy processors (Starita, 1999).

Internet Banking Platforms & Applications

Most of the Internet plumbing to present data onto Web interfaces from data sources is offered by Internet banking application software vendors, who link legacy systems to allow access to account data and transaction execution. Most players position themselves as end-to-end solution providers by including a proprietary front-end software product, integration with other front-end software, or Web design services.

Some of the solutions are middleware platforms with plug-in applications to provide bill payment, bill presentment, brokerage, loan, small business, and/or credit card functionality. Most vendors use Open Financial Exchange standard (OFX) to connect to different delivery channels such as Interactive Voice Response (IVRs), Personal Finance Managers (PFMs), and the Internet. Middleware tools are designed to handle Internet-delivered core banking and bill payment transaction (Walsh, 2002). Middleware platforms provide a link between financial institutions' legacy host systems and customers using browser-based HTML interfaces and OFX-enabled personal financial management software (Walsh, 2002).

Middleware is designed for financial institutions that require a platform that translates messages between collections of separate processing systems that house core processing functions. Core processing systems include bill payment, credit card, brokerage, loans and insurance. Electronic bill payment and presentment is widely believed to be the compelling application that brings large volumes of customers to the Internet channel to handle their finances. There are two kinds of Web sites: non-transactional and transactional. The non-transactional sites, commonly known as promotional Web sites, publish content with information about bank products and allow customers to investigate targeted areas such as college loans or retirement planning. These sites give basic information on bank products and do not allow any transactions. Banks can collect information to start to develop customer profiles by recording where a customer visits on the Web site and comparing it with demographic information to develop personalized marketing strategies.
Transactional sites link to back-end processing systems and include basic functionality such as the ability to view recent transactions and account histories, download information into Personal Financial Manager (PFM) software, and transfer funds between existing accounts. As banks become more sophisticated with transactional capabilities, such things as electronic bill payment or moving of funds outside of the bank become possible. Integrating with a third-party processor such as Checkfree or Travelers Express most often does this. Bill presentation is also part of transactional capability; however, it is being done on a limited basis through a small number of pilots. Some banks allow customers to apply for loans, mortgages, and other products online, although much of the back-end process is still done manually. In transactional Web sites, every page must be dynamically composed and offer continual updates on products and pricing.

**Standards Compliance**

Standards play a vital role in seamless flow and integration of information across channels and help in reducing risk emanating from diverse platforms and standards. In addition to the challenge of integrating Internet banking products into the bank’s own IT environment, many Internet banking functions involve third-party participation. This poses a significant integration question: What is the best way to combine separate technology systems with third parties in a cost-effective way to enable each participant to maintain control over its data, and maintain autonomy from other participants? The response from the technology marketplace has been to establish Internet banking standards to define interactions and the transfer of information between multiple parties (Bohle, 2001). The premise of a standard is that everyone would use it in the same consistent fashion; unfortunately, that is not the scenario in the current Internet banking environment. One of the problems for the lackluster performance of e-banking arguably is the industry’s failure to attend to the payments infrastructure (Orr, 2002). One initiative that does show promise is by the National Institute of Standards and Technology, that has developed a proposed standard, such as “Security Requirements for Cryptographic Modules,” that will require role based authentication and authorization (FIPS, 1992). Some of the standards pervasive in current e-banking models are the ADMS standard, the GOLD standard, and the OFX standard.

**INFORMATION ASSURANCE**

Web banking sites include financial calculators, e-mail addresses/customer service information, new account applications, transactions such as account balance checks, transfers, and bill payment, bill presentment/payment, cash management, loan applications, small business, credit card, and so forth. The modes by which they can be accessed include online service provider or portal sites, direct-dial PC banking program, Internet-bank Web sites, WebTV and personal financial manager. Depending on the functionality of the Web sites, different information assurance requirements are found.

Some examples of exploitation of information assurance issues in the Web banking arena include:

- Many ATMs of Bank of America were made unavailable in January 2003 by the SQL Slammer worm, which also affected other financial services like Washington Mutual.
- Barclays suffered an embarrassing in-
Table 1: Standards in E-Banking Models

- **The ADMS Standard**: Access Device Messaging System (ADMS) is a proprietary standard developed and supported by Visa Interactive. From September 1998, this standard has been made obsolete for GOLD standard.

- **The GOLD Standard**: The GOLD standard is an electronic banking standard developed and supported by Integrim to facilitate the exchange of information between participants in electronic banking transactions. Integrim is a PC direct-dial and Internet banking vendor developed as a consortium with 16 member banks, IBM and Visa Interactive (through acquisition) in an equal equity partnership. IBM is the technology provider for the Integrim consortium.

- **The OFX Standard**: Open Financial Exchange (OFX) is a standard developed cooperatively by Microsoft, Intuit and Checkfree. Recently, Microsoft launched its OFX version 2.0 without the involvement of its partners, Checkfree and Intuit. OFX v.2.0 is developed with XML to enable OFX to be used for bill presentment. Though OFX can be considered as a much better solution for inter-operability needs of banks, it imposes problems of incompatibility between older OFX versions.

- **The IFX Standard**: Interactive Financial Exchange (IFX) initiative was launched in early 1998 by BITs (the Banking Industry Technology Secretariat) in order to ensure convergence between OFX and another proposed specification, GOLD, propagated by Integrim Financial Network. According to the IFX forum, IFX specification provides a robust and scalable framework for the exchange of financial data and instructions independent of a particular network technology or computing platform.

- **XML as standard**: XML language is often perceived as a solution to the problem of standards incompatibility. XML appears as an ideal tool for multi-banking, multi-service Internet banking applications.

cident when it was discovered that after logging out of its online service, an account could be immediately re-accessed using the “back” button on a Web browser. If a customer accessed their Barclays account on a public terminal, the next user could thereby view banking details of the previous customer. According to the bank, when customers join the online banking service they are given a booklet that tells them to clear the cache to prevent this from happening. However, this procedure shifts the responsibility for security to the end user⁶.

**Security and Privacy Issues**

In their annual joint study in April 2002, the FBI and the Computer Security Institute noted that the combined financial losses for 223 of 503 companies that responded to their survey (Computer Crime and Security Survey) was $455 million for year 2002 (Junnarkar, 2002). Security and integrity of online transactions are among the most important technical issues that a bank offering Web services will need to tackle. The Internet bank Web sites handle security in different ways. They can choose either public or private networks. The Integrim consortium, for example, uses the private IBM/AT&T Global Network for all Internet network traffic (Walsh, 1999). Server security is another important issue, usually accomplished by server certificates and SSL authentication. Banks must look at three kinds of security (Walsh, 1999): communications security; systems security — from the applications/authorization server; information security.

From a user’s perspective, security must accomplish privacy, integrity authentication, access control, and non-repudiation. Security becomes an even more important issue when dealing with international banks, since only up to 128K encryption is licensed for export. Currently, most Internet

---

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
bank Web sites use a combination of encryption, firewalls, and communications lines to ensure security. The basic level of security starts with an SSL-compliant browser. The SSL protocol provides data security between a Web browser and the Web server, and is based on public key cryptography licensed from security systems. Security has been one of the biggest roadblocks that have kept consumers from fully embracing Internet banking. Even after the advent of highly secure sites with the aid of 128K encryption, a virtually invulnerable encryption technology, the perception among some consumers is that Internet banking is unsafe. They apprehend privacy violations, as the bank keeps track of all transactions, and they are unsure of who has access to privileged data about their personal net worth. The basic security concerns that face financial institutions offering banking services and products through the Internet are summarized in Figure 2 and are discussed next.

Authentication

Authentication relates to assurance of identity of person or originator of data. Reliable customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. Strong customer authentication practices are necessary to enforce “anti-money” laundering measures and help financial institutions detect and reduce identity theft. Customer interaction with financial institutions is migrating from physical recognition and paper-based documentation to remote electronic access and transaction initiation. The risks of doing business with unauthorized or masquerading individuals in an electronic banking environment could be devastating, which can result in financial loss and intangible losses like reputation damage, disclosure of confidential information, corruption of data or unenforceable agreements.

There is a gamut of authentication tools and methodologies that financial institutions use to authenticate customers.

---

Figure 2: E-Banking Security Infrastructure

![Diagram of E-Banking Security Infrastructure]

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
These include the use of passwords and Personal Identification Numbers (PINs), digital certificates using a Public Key Infrastructure (PKI), physical devices such as smart cards or other types of "tokens," database comparisons, and bio-metric identifiers. The level of risk protection afforded by each of these tools varies and is evolving as technology changes. Multi-factor authentication methods are more difficult to compromise than single factor systems. Properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents. Broadly, the authentication methodologies can be classified based on: what a user knows (password, PINs); what a user has (smart card, magnetic card); and what a user is (fingerprint, retina, voiceprint, signature).

The issues that face banks using the Internet as a channel are the risks and risk management controls of a number of existing and emerging authentication tools necessary to initially verify the identity of new customers and authenticate existing customers that access electronic banking services. Besides, effective authentication framework and implementation provides banks with a foundation to enforce electronic transactions and agreements.

- **Account Origination and Customer Verification:** With the growth in electronic banking and commerce, financial institutions need to deploy reliable methods of originating new customer accounts online. Customer identity verification during account origination is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. There are significant risks when financial institution accepts new customers through the Internet or other electronic channels because of the absence of the tangible cues that banks traditionally use to identify individuals (FDIC, 2001).

- **Monitoring and Reporting:** Monitoring systems play a vital role in detecting unauthorized access to computer systems and customer accounts. A sound authentication system should include audit features that can assist in the detection of fraud, unusual activities (e.g., money laundering), compromised passwords or other unauthorized activities (FDIC, 2001). In addition, financial institutions are required to report suspicious activities to appropriate regulatory and law enforcement agencies as required by 31 CFR 103.18.

**Access Control**

Access control refers to the regulating of access to critical business assets. Access control provides a policy-based control of who can access specific systems, what they can do within them, and when and from where they are allowed access. One of the primary modes of access control is based on roles. A role can be thought of as a set of transactions that a user or set of users can perform within the context of an organization. For example, the roles in a bank include teller, loan officer, and accountant, each of whom can perform different functions. Role-based access control (RBAC) policy bases access control decisions on the functions that a user is allowed to perform within an organization. In many applications, RBAC is concerned more with access to functions and information than strictly with access to information.

The applicability of RBAC to commercial systems is apparent from its widespread use. Nash and Poland (Poland & Nash, 1990) discuss the application of role-based access control to cryptographic authentication devices commonly used in the
banking industry. Even the Federal Information Processing Standard (FIPS) has provisions for support for role-based access and administration.

Non-Repudiation

Non-repudiation refers to the need for each party involved in a transaction to not go back on their word, that is, break the electronic contract (Pfleeger, 1997). Authentication forms the basis for non-repudiation. It requires strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents. This is important for an e-banking environment where, in all electronic transactions, including ATMs (cash machines), all parties to a transaction must be confident that the transaction is secure; that the parties are who they say they are (authentication), and that the transaction is verified as final. Essentially banks must have mechanisms that must ensure that a party cannot subsequently repudiate (reject) a transaction. There are several ways to ensure non-repudiation, which include digital signatures, which not only validates the sender, but also "time stamps" the transaction, so it cannot be claimed subsequently that the transaction was not authorized or not valid.

Integrity

Ensuring integrity means maintaining data consistency and protecting from unauthorized data alteration (Pfleeger, 1997). Integrity is very critical for Internet banking applications, as transactions have information that is consumer and business sensitive. To achieve integrity, data integrity mechanisms can be used. These typically involve the use of secret-key or public-key based algorithms that allow the recipient of a piece of protected data to verify that the data have not been modified in transit. The mechanisms are further presented in a later section.

Confidentiality and Privacy

Privacy and security concerns are not unique to banking systems. Privacy and confidentiality are related but are distinct concepts. Protection of personally identifiable information like banking records must be ensured before consumers. Information Privacy (NIHAC, 1995) is the ability of an individual to control the use and dissemination of information that relates to him or her. Confidentiality (NIHAC, 1995) is a tool for protecting privacy. Sensitive information is accorded a confidential status that mandates specific controls, including strict limitations on access and disclosure. Those handling the information must adhere to these controls. Information confidentiality refers to ensuring that customer information is secured and hidden as it is transported through the Internet environment. Information must not only be protected wherever it is stored (e.g., on computer disks, backup tape and printed form), but also in transit through the Internet.

Availability

Availability in our context means that legitimate users have access when they need it. With Internet banking, one of the strongest selling propositions is 24x7 availability; therefore it becomes even more critical for e-banks. Availability applies to both data and to services. Expectations of availability include presence of a service in usable form, capacity to meet service needs, timeliness of service, fair allocation, fault tolerance, controlled concurrency and deadlock management. One example where availability is compromised is the

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
denial of service attack. On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. When there are enormous transactions on the Internet bank’s Web site, the losses that may arise owing to unavailability are severe, in terms of financial losses and reputation losses. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. It becomes imperative and crucial for IT managers in the Internet banking world to better understand the kind of denial of attacks possible. Some of the common and well-known types of denial of service attacks (IESAC, 2003) are:

- **SYN Attack**: It floods the server with open SYN connections, without completing the TCP handshake. TCP handshake is a three-step process to negotiate connection between two computers. The first step is for initiating computer to send “SYN” (for “synchronize”) packet.
- **Teardrop Attack**: It exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. Here, the attacker’s IP puts a confusing offset value in the second or later fragment of the packet. It can cause the system to crash.
- **Smurf Attack**: In this attack, the perpetrator spoofs the source IP address and broadcasts ping requests to multitude of machines to overwhelm the victim.

**Perimeter Defense**

Perimeter defense refers to the separation of an organization’s computer systems from the outside world (IETF, 2000). This must allow free sharing of certain information with clients, partners, suppliers and so on, while also protecting critical data from them. A security bulwark around network and information assets of any bank can be achieved, to a certain extent, by implementing firewalls and correctly performing tuning and configuration of firewalls.

Today, with the kind of traffic generated towards Web-banking sites for all kinds of purposes, from balance enquiries to Inter-bank fund transfers, implementation of screening routers to ensure incoming and outgoing traffic would add another layer of security. In this age of systems being hijacked for cyber-attacks, it is also important that screen routers detect and prevent outgoing traffic that attempts to gain entry to systems like spoofing IP addresses. Further, the periphery of the corporate computer infrastructure can be bolstered by implementing VPN solutions to ensure privacy of data flowing through the firewall into the public domain.

Probes and scans are often used techniques that are exploited to learn about exposures and vulnerabilities on the network systems. A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion. A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a mis-configuration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

**Intrusion Detection**

Intrusion detection refers to the ability to identify an attempt to access systems and networks in a fashion that breaches security policies. The Internet banking sce-
nario, where most of business these days is carried out over public domain Internet and where a banking Web site becomes a single point interface for information as well as transactions, gives hackers enough motivation to intrude into Internet banks’ systems. To safeguard from such unwanted activities, organizations need to be able to recognize and distinguish, at a minimum, the following (Gartner, 1999): internal & external intrusion attempts; human versus automated attacks; unauthorized hosts connecting to the network from inside and outside the perimeter; unauthorized software being loaded on systems; and all access points into the corporate network.

Intrusion detection systems (IDS) allow organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be whether to use intrusion detection, but which intrusion detection features and capabilities to use. IDSs have gained acceptance as a necessary addition to every organization’s security infrastructure. IDS products can provide worthwhile indications of malicious activity and spotlight security vulnerabilities, thus providing an additional layer of protection. Without them, network administrators have little chance of knowing about, much less assessing and responding to, malicious and invalid activity. Properly configured, IDSs are especially useful for monitoring the network perimeter for attacks originating from outside and for monitoring host systems for unacceptable insider activity.

Security Event Detection

Security event detection refers to the use of logs and other audit mechanisms to capture information about system and application access, types of access, network events, intrusion attempts, viruses, and so forth.

Logging is an important link in analysis of attack and real-time alerts of any kind of suspicious activity on the Internet bank Web site. For proper tracking of unusual events and attempts of intrusion, the following logs should be collected: basic security logs, network event logging, log authentication failures, log access violations, log attempts to implant viruses and other malicious code, and log “abnormal” activity. This strongly implies that the technical department that is analyzing logs to identify “unusual behavior” must be aware of business initiatives. Besides, it has to be ensured that audit logs are retained long enough to satisfy legal requirements. Also, at a minimum, investigation of security breaches should be allowed for up to 14 days after any given attack (IETF, 2000). Today, data mining techniques can interpret millions of items of log data and reveal any unobserved attempts to breach an e-bank’s Web site. For this it has to be ensured that logs do not overwrite themselves causing loss of data. For analysis of events at a site, documentation of automated systems that identify what the logs mean should be maintained. Understanding the nature of attempts such as whether an attack was from within the organization or from outside or whether it was just a false alarm is critical to security.

Malicious Content

Malicious content refers to programs of any type that are introduced into a system to cause damage or steal information. Malicious content includes viruses, Trojans, hacker tools, and network sniffers. While common in multiple domains, this is as important in the e-banking world as well. Malicious code brings with it the potential
to create serious technical and economic impact by crashing e-mail servers and networks, causing millions of dollars of damage in lost productivity.

Some of the common forms of malicious contents are:

- **Virus:** A virus is a computer program that runs on a system without being asked to do so, created to "infect" other computer programs with copies of itself. Pioneer virus researcher Fred Cohen has defined a virus as "a program that can 'infect' other programs by modifying them to include a, possibly evolved, copy of it".

- **Worm:** A worm has the ability to spread over a network and, thus, can take advantage of the Internet to do its work. Worms reside in memory and duplicate themselves throughout the network without user intervention.

- **Trojan Horse:** Trojan horse is the name applied to malicious computer program disguised as a seemingly innocent activity such as initiating a screen saver, accessing an e-mail attachment, or downloading executable files from an untrusted Web site. Some of the widely manifested malicious codes are Stoned, Yankee, Michelangelo, Joshi, Lehigh, Jerusalem, MBDF (for Macintosh), Melissa, Concept, LoveBug (ILOVEYOU), ShapeShift, Fusion, Accessiv, Emporer, Sircam, Nimda, Badtrans.

Protection against malicious codes like viruses, worms, Trojan horses, and so forth could be effectively dealt with by installing security protection software that thwarts and mitigates the effects of codes.

However, such software provides only a level of defense and is not by itself sufficient. Recommendations for e-banking IT infrastructure include (Noakes, 2001):

- Install detection and protection solutions for all forms of malicious code, not just an antivirus solution.
- Ensure that all users are aware of and follow safe behavior practices — do not open attachments that have not been scanned, do not visit un-trusted Web sites, and so forth.
- Ensure that users are aware of how easy data may be stolen automatically just by visiting a Web site. Install an effective solution. Keep it current with the latest signatures as new forms of malicious code are identified.
- Use anti-spammers, harden operating systems, configure stricter firewall rules, and so forth.

### Security Services, Mechanisms & Security Protection

Security risks are unlike privacy risks; they originate outside the Financial Service Provider (FSP) and change rapidly with advances in technology (DeLotto, 1999). In December 2000, IATF released guidelines that require all covered institutions to secure their clients’ personal information against any "reasonably foreseeable" internal or external threats to their security, confidentiality and integrity. By July 1, 2001, FSPs were expected to develop customer information security programs that: ensured the security and confidentiality of customer information, protected against any anticipated threats or hazards to the security or integrity of customer information, and protected against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.

The services and mechanisms that are prevalent in an e-banking environment are presented below in order to provide an understanding of key issues and terms in-
volved.

**Encryption**

Encryption is the process of using a key to scramble readable text into unreadable cipher-text. Encryption on the Internet in general, and e-banking, in particular, has many uses, from the secure transmission of credit card numbers via the Web to protecting the privacy of personal e-mail messages. Authentication also uses encryption, by using a key or key pair to verify the integrity of a document and its origin. The Data Encryption Standard (DES) has been endorsed by the National Institute of Standards and Technology (NIST) since 1975 and is the most readily available encryption standard. Rivest, Shamir and Adleman (RSA) encryption is a public-key encryption system, is patented technology in the United States, and thus is not available without a license. RSA encryption is growing in popularity and is considered quite secure from brute force attacks. Another encryption mechanism is Pretty Good Privacy (PGP), which allows users to encrypt information stored on their system as well as to send and receive encrypted e-mail. Encryption mechanisms rely on keys or passwords. The longer the password, the more difficult the encryption is to break. VPNs employ encryption to provide secure transmissions over public networks such as the Internet.

**Security Protocol Services**

The Internet is viewed as an insecure place. Many of the protocols used in the Internet do not provide any security. Today's businesses, particularly the banking sector, must integrate security protocols into their e-commerce infrastructure to protect customer information and privacy. Some of the most common protocols are briefly discussed in Appendix A.

**Firewalls & Intrusion Detection Systems**

A firewall is a collection of hardware and software designed to examine a stream of network traffic and service requests. Its purpose is to eliminate from the stream those packets or requests that fail to meet the security criteria established by the organization. A simple firewall may consist of a filtering router, configured to discard packets that arrive from unauthorized addresses or that represent attempts to connect to unauthorized service ports. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state. But a firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether (Odyssey, 2001). In this age of systems being hijacked, it is also important that firewalls and screen routers detect and prevent outgoing traffic that attempts to compromise the integrity of the systems.

A Network Intrusion Detection System (NIDS) analyzes network traffic for attacks. It examines individual packets within the data stream to identify threats from authorized users, backdoor attacks and hackers who have thwarted the control systems to exploit network connections and access valuable data. NIDS add a new level of visibility into the nature and characteristics of the network. They provide information about the use and usage of the network. Host Based IDS/Event Log Viewers are a kind of IDS that monitors event logs from multiple sources for suspicious activity. Host IDS are best placed to detect computer misuse from trusted insiders.
and those who have infiltrated the network.

The technology and logical schemes used by these systems are often based on *knowledge-based misuse detection* (Allan, 2002). Knowledge-based detection methods use information about known security policy, known vulnerabilities, and known attacks on the systems they monitor. This approach compares network activity or system audit data to a database of known *attack signatures* or other misuse indicators, and pattern matches produce alarms of various sorts. Behavior-based detection (Allan, 2002) methods use information about repetitive and usual behavior on the systems they monitor. Also called *anomaly detection*, this approach notes events that diverge from expected (based on repetitive and usual) usage patterns. One technique is *threshold detection* (Allan, 2002), in which certain attributes of user and system behavior are expressed in terms of counts, with some level established as permissible. Another technique is to perform *statistical analysis* (Allan, 2002) on the information, build statistical models of the environment, and look for patterns of anomalous activity.

**Passwords & Personal Identification Numbers (PINs)**

The most common authentication method for existing customers requesting access to electronic banking systems is the entry of a user name and a secret string of characters such as a password or PIN. User IDs combined with passwords or PINs are considered a single-factor authentication technique. There are three aspects of passwords that contribute to the security they provide: secrecy, length and composition, and system controls. In the present Internet banking scenario, there are policies, for both customers as well as employees, set by banks for passwords to ensure effective authentication, like prohibiting using public e-mail IDs as user IDs, ensure that there are no user IDs with no password, ensure that policies exist and can be automatically enforced concerning minimum password length, password format (which characters make up a valid password), expiration and renewal of passwords, uniqueness of passwords, not allowing the use of “real” words for passwords, and so forth.

**Tokens**

The use of a token represents authentication using “something the customer possesses”. Typically, a token is part of a two-factor authentication process, complemented by a password as the other factor. There are many benefits to the use of tokens. The authentication process cannot be completed unless the device is present. Static passwords or biometric identifiers used to activate the token may be authenticated locally by the device itself. This process avoids the transmission of shared secrets over an open network such as the Internet.

**Digital Certificates & Public Key Infrastructure (PKI)**

A financial institution may use a PKI system to authenticate customers to its own electronic banking product. Institutions may also use the infrastructure to provide authentication services to customers who wish to transact business over the Internet with other entities or to identify employees and commercial partners seeking access to the business’s internal systems. A properly implemented and maintained PKI may provide a strong means of customer identification over open networks such as the Internet. By combining a variety of hardware components, system software, policies, practices, and standards, PKI can pro-
vide for authentication, data integrity, and defenses against customer repudiation, and confidentiality (Odyssey, 2001). The certificate authority (CA), which may be the financial institution or its service provider, plays a key role by attesting with a digital certificate that a particular public key and the corresponding private key belong to a specific individual or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of customers is adequately controlled. The CA attests to the individual’s identity by signing the digital certificate with its own private key, known as the root key. Each time the customer establishes a communication link with the financial institution, a digital signature is transmitted with a digital certificate. These electronic credentials enable the institution to determine that the digital certificate is valid, identify the individual as a customer, and confirm that transactions entered into the institution’s computer system were performed by that customer. PKI, as the most reliable model for security and trust on the Internet, offers a comprehensive e-security solution for Internet banking. Unlike the other security models, PKI is a standards compliant, most credible trust framework, highly scalable and modular. PKI comprehensively satisfies the security requirements of e-banking (Odyssey, 2001).

A brief discussion on the processes and mechanisms used in PKI to address common security concerns follows:

- **Authentication**: The customer requests the Registration Authority (RA) for a certificate. The Registration Authority validates the customer’s credentials. After valid credentials are ensured, the RA passes the certificate request to the Certification Authority (CA). CA then issues the certificates. A digital certificate can be stored on the browser on the user’s computer, on a floppy disk, on a smart card or on other hardware tokens.

- **Confidentiality**: The customer generates a random session key at his or her end. The session key is sent to the bank, encrypting it with the bank’s public key. The bank decrypts the encrypted session key with its private key. The session key is employed for further transactions.

- **Integrity**: The message is passed through a suitable hashing algorithm to obtain a message digest or hash. The hash, encrypted with the sender’s private key, is appended to the message. The receiver, on receiving the message, passes it through the same hashing algorithm. The digest he or she obtains is compared with the received and decrypted digest. If the digests are same, it implies that the data have not been tampered with in transit.

- **Non-Repudiation**: The hash is encrypted with the sender’s private key to yield the sender’s digital signature. Since the hash is encrypted with the sender’s private key (which is accessible only to him or her), it provides an indisputable means of non-repudiation.

- The use of digital signatures and certificates in Internet banking has provided the trust and security needed to carry out banking transactions across open networks like the Internet. PKI, being a universally accepted standards compliant security model, provides for the establishment of a global trust chain (Odyssey, 2001).

**Biometrics**

A biometric identifier measures an individual’s unique physical characteristic or behavior and compares it to a stored digital template to authenticate that individual.
A biometric identifier representing "something the user is" can be created from sources such as a customer's voice, fingerprints, hand or face geometry, the iris or retina in an eye, or the way a customer signs a document or enters keyboard strokes (FDIC, 2001). The success of a biometric identifier rests on the ability of the digitally stored characteristic to relate typically to only one individual in a defined population. Although not yet in widespread use by financial institutions for authenticating existing customers, biometric identifiers are being used in some cases for physical access control.

Banks could use a biometric identifier for a single or multi-factor authentication process. ATMs that implement biometrics like iris-scan technologies are examples of the use of a biometric identifier to authenticate users. The biometric identifier may be used for authentication, instead of the PIN. A customer can use a PIN or password to supplement the biometric identifier, making it part of a more secure two-factor authentication process. Financial institutions may also use biometric identifiers for automating existing processes. Another application would be a financial institution that allows customer to reset a password over the telephone with voice-recognition software that authenticates the customer. An authentication process that relies on a single biometric identifier may not work for everyone in a financial institution's customer base. Introducing a biometric method of authentication requires physical contact with each customer to initially capture the physical identifier, which further buttresses the initial customer verification process. But this process may increase the deployment costs.

**Hardware Security Devices (HSDs)**

This mechanism is an extension to usage of tokens for authentication. Using hardware devices for authentication provide "hacker-resistant" and "snooping-proof" two-factor authentication, resulting in easy-to-use and effective user identification (Grand, 2001). To access protected resources, the user simply combines his or her secret PIN (something he or she knows) with the code generated by his or her token (something he or she has). The result is a unique, one-time-use code that is used to positively identify, or authenticate the user (Grand, 2001). Some central server validates the code. Goal: provide acceleration, secure key management. A hardware security module is a hardware-based security device that generates stores and protects cryptographic keys.

There are universal criteria for rating these devices. The criteria are documented in a Federal Information Processing Standard (FIPS) called FIPS 140-1 to 140-4 — Security for Cryptographic Modules. Such hardware devices generate tokens that are dynamic one-time passwords, through the use of a mathematical function. Passwords generated by tokens are different each time the user requests one, so an intercepted password is useless as it will never be used again. Acceptance and credibility of the devices is reflected in the increasing number of devices in use.

**Industry Standards & Frameworks**

Industry standards for financial transactions over the Internet are an absolute necessity for ensuring various security aspects of business as well as consumer confidence. There has been a constant search and development of standards for e-banking infrastructural tenets like authentication, access control, non-repudiation, and so forth. Some of the standards developed and advocated by different industry players and their proponents are briefly discussed in
Table 2: End-User Involvement with the Security Issues

<table>
<thead>
<tr>
<th>Security issues with direct user focus</th>
<th>User-focused mechanisms that are available</th>
<th>User-transparent mechanisms/technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Passwords, PINs, tokens, HSDs, Biometrics</td>
<td>Radios, TACACS, PKI, ISAKMP</td>
</tr>
<tr>
<td>Access Control</td>
<td>Roles, User Discretion, Hard-coded systems</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Training</td>
<td>Encryption</td>
</tr>
<tr>
<td>Integrity</td>
<td>Encryption (hashing)</td>
<td></td>
</tr>
<tr>
<td>Malicious Content</td>
<td>Training</td>
<td>Mail/Span filters, anti-virus</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Use of PKI, and authentication mechanisms</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>Training</td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Training</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security issues with system-only focus</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>IDSs, Firewall, redundancy, fault-tolerance, application-level security rules</td>
</tr>
<tr>
<td>Security Event, Intrusion Detection</td>
<td>IDSs, probes, firewalls</td>
</tr>
<tr>
<td>Perimeter Defense</td>
<td>Firewalls, IDSs</td>
</tr>
<tr>
<td>Administration</td>
<td>Depends on the system policies as well as administrators.</td>
</tr>
</tbody>
</table>

Appendix B for overall understanding of the evolution and prevalence of some of the standards.

To summarize, Table 2 presents issues that user has direct control on or involvement with and issues that are commonly left for the systems to handle.

CONCLUSIONS

It should be noted that the discussion of e-banking information assurance (IA) issues has also included several generic IA issues. To illustrate this, Table 3 briefly categorizes e-banking specific information assurance issues and generic issues separately. Some issues may be more significant than in other areas. We have made an attempt to comprehensively discuss all the areas in the article.

Security for financial transactions is of vital importance to financial institutions providing or planning to provide service delivery to customers over the public Internet, as well as to suppliers of products, services, and solutions for Internet-based e-commerce. The actual and perceived threats to Internet-based banking define the need for a set of interrelated security services to provide protection to all parties that can benefit from Web banking in a secure environment. Such services may be specific to counter particular threats or may be pervasive throughout an Internet based environment to provide the levels of protection needed.

There are also requirements that the entire e-commerce environment be constructed from components that recognize the need for security services and provide means for overall security integration, administration, and management. These services that offer the security from an infrastructure standpoint are found throughout

Table 3: IA Issues

<table>
<thead>
<tr>
<th>E-banking Specific Issues</th>
<th>Generic Issues in E-banking</th>
</tr>
</thead>
</table>
the e-commerce network and computing infrastructure. Financial institutions should carry out, as a matter of corporate security policy, identification of likely targets, which should include all systems that are open to the public network, such as routers, firewalls, and Web servers, modern banks' Web sites, and internal unsecured systems such as desktops. They should regularly revise and update their policies on auditing, risk assessment, standards, and key management. Vulnerability assessment and identification of likely targets and the recognition of systems most vulnerable to attack are critical in the e-banking arena. Accurate identification of vulnerable and attractive systems will contribute to prioritization when addressing problem areas.

ACKNOWLEDGMENTS

The authors would like to thank John Walp and Shamik Banerjee for their contributions and help with the paper, and the anonymous referees for their comments that have improved the paper. We would also like to thank the NSA for the Center for Information Assurance recognition and Department of Defense for two student fellowships. The research of the second author was supported in part by National Science Foundation (NSF) under grant 990735 and the research of the third author was supported in part by U.S. Air Force Research Lab, Rome, New York under Contract F30602-00-10505.

REFERENCES


Basel Committee. (2001). Risk man-

gement principles for electronic banking. Basel Committee publications No. 82.


Internet Security Task Force. (2000). Initial recommendations for conducting se-


ENDNOTES

2 http://www.orcc.com
6 The latest version of the specifications, EMV 2000 version 4.0, was published in December 2000 (http://www.emvco.com/).
7 CEN/ISSS was created in mid-1997 by CEN (European Committee for Stan-
APPENDIX A

(Common Security Protocol Services)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>Originally developed by Netscape, the SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. SSL has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. However, SSL consumes large amounts of the Web server’s processing power due to the massive cryptographic computations that take place when a secure session is initiated. If many secure sessions are initiated simultaneously, then the Web server quickly becomes overburdened. The results are slow response times, dropped connections, and failed transactions.</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>SSH Secure Shell is the de facto standard for remote logins. It solves an important security problem on the Internet of password hacking. Typical applications include secure use of networked applications, remote system administration, automated file transfers, and access to corporate resources over the Internet.</td>
</tr>
<tr>
<td>AS1 and AS2</td>
<td>AS1 provides security over SMTP(Simple Mail Transfer Protocol) through object signature and object encryption technology. AS2 goes a step further than AS1 by supporting S/MIME over HTTP and HTTPS. Both AS1 and AS2 provide data authentication, proving that the sender and receiver are indeed the people or company that they claim to be.</td>
</tr>
<tr>
<td>Digital Certificates</td>
<td>Digital certificates are used to authenticate the identity of trading partners, ensuring partners are really who they say they are. In addition to data authentication, digital signatures support non-repudiation, proving that a specific message did come from a known sender at a specific time. A digital signature is a digital code that can be sent with electronically transmitted message and it uniquely identifies the sender. It is based on digital certificates. This prevents partners from claiming that they did not send or receive a particular message or transaction.</td>
</tr>
<tr>
<td>Pretty Good Privacy (PGP)</td>
<td>PGP is a freely available encryption program that uses public key cryptography to ensure privacy over FTP, HTTP and other protocols. PGP is the de-facto standard software for the encryption of e-mail and works on virtually every platform. But PGP suffers from absence of trust management and it is not standards compliant, though it could provide for integrity, authentication, non-repudiation and confidentiality. PGP also provides tools and utilities for creating, certifying, and managing keys.</td>
</tr>
<tr>
<td>Secure Multipurpose Internet Mail Extension (S/MIME)</td>
<td>S/MIME addresses security concerns such as privacy, integrity, authentication and non-repudiation, through the use of signed receipts. S/MIME provides a consistent way to send and receive secure MIME data. Based on the MIME standard, S/MIME provides authentication, message integrity, non-repudiation of origin (using digital signatures) and data confidentiality (using encryption) for electronic messaging applications. Since its development by RSA in 1996, S/MIME has been widely recognized and a widely used standard for messaging. The technology for S/MIME is primarily built on the Public Key Cryptographic Standard, which provides cryptographic interoperability. Two key features of S/MIME are the digital signature and the digital envelope. Digital signatures ensure that a message has not been tampered with during transit. Digital signatures also provide non-repudiation so senders cannot deny that they sent the message.</td>
</tr>
<tr>
<td>Secure HTTP (S-HTTP)</td>
<td>S-HTTP is an extension to HTTP, which provides a number of security features, including Client/Server Authentication, Spontaneous Encryption and Request/Response Non-repudiation. S-HTTP allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL). A major difference is that S-HTTP allows the client to send a certificate to authenticate the user, whereas using SSL, only the server can be authenticated. S-HTTP is more likely to be used in situations where the server represents a bank and requires verification from the user that is more secure than a user id and password.</td>
</tr>
<tr>
<td>Simple Key management for Internet Protocols (SKIP)</td>
<td>It is a manifestation of IP-Level Cryptography that secures the network at the IP packet level. Any networked application gains the benefits of encryption, without requiring modification. SKIP is unique in that an Internet host can send an encrypted packet to another host without requiring a prior message exchange to set up a secure channel. SKIP is particularly well suited to IP networks, as both are stateless protocols.</td>
</tr>
<tr>
<td>Encapsulating Security Payload (ESP)</td>
<td>ESP is security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. ESP completely encapsulates user data. ESP can be used either by itself or in conjunction with AH. ESP may be implemented with AH, as discussed in next paragraph, in a nested fashion through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host, depending on the implementation. ESP may be used to provide the same security services, and it also provides a confidentiality (encryption) service. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode).</td>
</tr>
<tr>
<td>Authentication Header (AH)</td>
<td>A security protocol that provides authentication and optional replay-detection services. AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used either by itself or with Encapsulating Security Payload (ESP). The IP Authentication Header is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays. AH provides authentication for as much of the IP header as possible, as well as for upper layer protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is somewhat piecemeal and not complete.</td>
</tr>
</tbody>
</table>

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
### APPENDIX B

(Some Industry Standards & Frameworks in E-Banking)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SET</td>
<td>Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wafer (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape’s Secure Sockets Layer (SSL), Microsoft’s Secure Transaction Technology (STT), and Terisa System’s Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI). SET provides authentication, integrity, non-repudiation and confidentiality.</td>
</tr>
<tr>
<td>HBMS</td>
<td>HBMS is a specification for the communication between intelligent customer systems and the corresponding computing centers for the exchange of home banking transactions. The transmission of data is done by a net data interface, which is based on flexible definer syntax.</td>
</tr>
<tr>
<td>EMV</td>
<td>Specifications by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used.</td>
</tr>
<tr>
<td>CEPS</td>
<td>The Common Electronic Purse Specifications (CEPS) define requirements for all components needed by an organization to implement a globally interoperable electronic purse program, while maintaining full accountability and auditability. CEPS, which were made available in March of 1999, outline overall system security, certification and migration. CEPS have paved the way for the creation of an open, de facto, global electronic purse standard (<a href="http://www.ceps.org/">http://www.ceps.org/</a>).</td>
</tr>
<tr>
<td>XMLPay</td>
<td>XMLPay is a standard proposed/developed by Ariba and Vertitan. It defines an XML syntax for payment transaction requests, responses and receipts in a payment processing network. The intended users are Internet merchants and merchant aggregators who need to deal with multiple electronic payment mechanisms (credit/debit card, purchase card, electronic check and automated clearing house payment). The supported operations include funds authorization and capture, sales and return sales, and voiding of transactions.</td>
</tr>
<tr>
<td>ECML</td>
<td>The Electronic Commerce Modeling Language ECML is a specification that describes the format for data fields that need to be filled at checkout in an online transaction. The fields defined include shipping information, billing information, recipient information, payment card information and reference fields. Version 2.0 describes these fields in XML syntax.</td>
</tr>
<tr>
<td>W3C standard on micropayments</td>
<td>The W3C standard on micropayments has originated from BM’s standardization efforts. It covers the payment function for payment of digital goods. The micropayment initiative specifies how to provide in a Web page all the information necessary to initiate a micropayment and transfer this information to the wallet for processing. The W3C Ecommerce/Micropayment Activity is now closed.</td>
</tr>
<tr>
<td>Passport</td>
<td>Microsoft Passport is an online user-authentication service. Passport’s primary service is user authentication, referred to as the Passport single sign-in (SSO) service. Passport also offers two other optional services: Passport express purchase (EP), which lets users store credit card and billing/shipping address information in their optional Passport wallet profiles to expedite checkout at participating e-commerce sites, and Kids Passport (source: Microsoft Passport Technical White Paper).</td>
</tr>
<tr>
<td>eWallet project of CEN/ISSSS</td>
<td>CEN/ISSSS Electronic Commerce Workshop initiated the eWallet project in mid-2001 assuming a need for standardization in the field. CEN/ISSSS has chosen a flexible working definition, considering an eWallet as &quot;a collection of confidential data of a personal nature or relating to a role carried out by an individual, managed so as to facilitate completion of electronic transactions.&quot;</td>
</tr>
<tr>
<td>SEMPER</td>
<td>Secure Electronic Market Place for Europe (SEMPER) was produced by an EU supported project under a special program, undertaken by a 20-partner consortium led by IBM. It is a definition of an open and system independent architecture for electronic commerce. The project was concluded in 1999. Based on access via a browser, the architecture specifies common functions to be supported by applications, which include exchange of certificates, exchange of signed offer/bid, fair contract signing, fair payment for receipt, and provision of delivery information.</td>
</tr>
<tr>
<td>IOTP</td>
<td>The Internet Open Trading Protocol (IOTP) is defined as an interoperable framework for Internet commerce. It is optimized for the case where the buyer and the merchant do not have a prior acquaintance. IOTP is payment system independent. It can encapsulate and support several of the leading payment systems.</td>
</tr>
<tr>
<td>SEPP</td>
<td>Secure Electronic Payment Process is a protocol developed by MasterCard and Netscape to provide authentication, integrity and payment confidentiality. It uses DES for confidentiality and 512, 768, 1024 or 2048-bit RSA and 128 bit MD5 hashing. RSA encrypts DES key to encrypt hash of account numbers. It uses up to three public keys, one for signing, one for key exchange, and one for certificate renewal. Besides, SEPP uses X.509 certificates with CMS at top of hierarchy [26].</td>
</tr>
<tr>
<td>STT</td>
<td>Secure Transaction Technology was developed by Visa and Microsoft to provide authentication, integrity and confidentiality to the Internet based transactions. It is based on 64-bit DES or 64-bit RC4 (24-bit salt) for confidentiality and 512, 768, 1024 or 2048-bit RSA for encryption with 160-bit SHA hashing. Its uses two public keys, one for signing, and one for key exchange. It has credentials similar to certificates but with account details and higher-level signatures, though they are not certificates.</td>
</tr>
<tr>
<td>JEPJ</td>
<td>(Joint Electronic Payment Initiative) CommerceNet and the W3 Consortium are jointly initiating a multi-industry project to develop an Internet payment negotiation protocol. The project explores the technologies required to provide negotiation over multiple payment instruments, protocols and transports. Examples of payment instruments include credit cards, debit cards, electronic cash and checks. Payment protocols include STT and SEPP (amongst others). Payment transport encompasses the message transmission mechanism: S-HTTP, SSL, SMTP, and TCP/IP are all categorized as transport technologies that can be used for payment.</td>
</tr>
</tbody>
</table>

---

Copyright © 2001, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Manish Gupta is an executive at M&T Bank in the Information Security Division. He recently graduated from SUNY Buffalo with an MBA.

H. Raghav Rao is a professor of MIS and an adjunct professor of CSE at SUNY Buffalo.

S. Upadhyaya is an associate professor of CSE and director of the Center of Excellence in Information Systems Assurance Research and Education at SUNY Buffalo.