Implications of Internet Technology: On-Line Auditing and Cryptography

BY ALEXANDER KOGAN, EPHRAIM F. SUDIT AND MIKLOS A. VASARHELYI

The auditing profession is significantly affected by cyberspace developments. In this article we focus on two important aspects: the opportunities for continuous on-line auditing through the Internet and the cryptographic technology that makes the necessary security arrangements possible.

Continuous on-line distance auditing

Continuous process auditing is an advanced audit process which a large percentage of the audit is automated and continuous. The key concepts involved were developed at AT&T Bell Laboratories for the AT&T internal audit organization where the continuous process auditing (CPA) system was actually implemented.

The objectives of continuous process auditing are to provide an integrated diagnostic view of an on-line, real-time system, to monitor the system in order to provide early warning of system problems (e.g. control weaknesses), and to ensure the financial integrity of the system. A continuous process audit system, then, is a system built to support these tasks and allow the auditor to do this in as much detail as she or he wanted. Additionally, the system should provide access to traditional and advanced audit evaluation tools.

In continuous process auditing, data flowing through the system are monitored and analyzed continuously (e.g. daily) using a set of auditor defined rules. Exceptions to these rules will trigger alarms that are intended to call the auditor's attention to any deterioration or anomalies in the system. CPA amounts to an analytical review technique since constantly analyzing process auditing can be considered as a meta form of control and can be used in monitoring control (compliance) either directly, by looking for electronic signatures, or indirectly by scanning for the occurrence of certain patterns or specific events. Ultimately, if a system is monitored over time, using a set of auditor heuristics, the audit can rely mainly on exception reporting and the auditor is called in only when exceptions arise. Many different types of auditor heuristics can be gathered to be "wired" into the CPA system (e.g. via SQL queries to a database and further manipulation, if necessary). The examples below are representative of exceptions, but generic in nature:

- If there is an increase in telephone traffic of 20 percent over a period, expect an increase of similar size in billing 20 days from that day. Investigate if more than 5 percent variance.
- If the total number of errors dropped by edits is larger than 2 percent of transactions, then investigate error type break down.
- If there is a sudden large drop (in a day) of the size of the retained error file, then an error correction audit is necessary.

"continuous process auditing is to provide an integrated diagnostic view of an on-line real-time system and to monitor the system in order to provide early warnings."

Impounding the auditor function into the system means tests that would normally be performed once a year are repeated daily.

The impact of the Internet

The advent of the Internet changed considerably the cost/benefit tradeoffs of an audit. With the advent of the World Wide Web (WWW) and its bandwidth demanding technology, we also find paths and common technologies that further open the road an entire new set of opportunities opens up with the advent and the culture of open networking.[1, 2, 3, 4] Part of this forthcoming line of action is described in *Continuous Control Monitoring (CCM)*,[5] where the basic CPA system setup is expanded by a combination of manual and automated controls of controls as well as analytic schemata to deal with control aggregation and analysis.

Opportunities

Considering the new environment, cost/benefit tradeoffs and opportunities are appearing for continuous audit such that:

- Computers can be monitored without direct on-line connectivity;
- Log files can be browsed remotely without expensive software adaptation;
- Large and small machines can interface seamlessly;
- Source document images can be examined from any auditor location;
- "Audit Servers" can be set up at very low cost for remote monitoring using ready-to-use Internet technology;
- Intranets can serve as main conduits for audit work and protect internal systems;
- Electronic signatures and authentication can progressively replace manual processes; and
- Process observation can be made continuous through the use of technologies like "CU SeeMe" where a narrow bandwidth is used for observation (static) over voice communication, or as a supplement to physical inventory counts.

> *"The Internet provides a technical possibility of transforming external audits from periodic to continuous."*

Figure 1 — CCM as a Modified CPA System Architecture

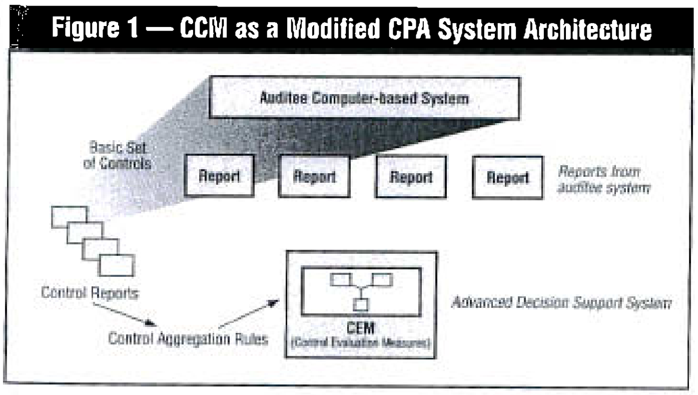
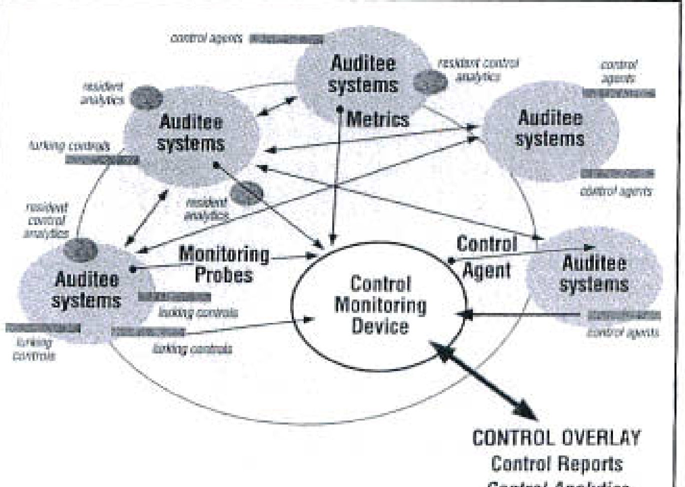

Auditee Computer-based System
Basic Set of Controls
Report
Report
Report
Report
Reports from auditee system
Control Reports
Control Aggregation Rules
CEM (Control Evaluation Measures)
Advanced Decision Support System

Figure 2 — Distributed and Internetworked Systems: Control Overlays



The Internet provides a technical possibility of transforming external audits from periodic to continuous. This may be a controversial issue since auditees may resist the rigor of continuous exposure. On the other hand, continuous auditing is likely to increase compliance and reduce incidences of "creative accounting" or incidents of negligence in performing controls.

CPAS & CCM

The five basic elements of the CPAS effort (measurement, metrics, analytics, alarms and standards) as well as the enhancements in CCM (control monitoring, measurement, indices and evaluation) will be affected by these new factors.

The CPAS implementation uses measurement as opposed to monitoring in capturing data for its processes. The difference is that CPAS relied on secondary data (e.g. reports) instead of directly measured (probed) items. Metrics are measures of particular system variables captured from reports or probes. Analytics link metrics with standards, other metrics, formulae and heuristics in evaluating system performance. Alarms are used to warn of significant differences between metrics and standards.

The CPAS effort uses document extraction, e-mailing, transmission and distillation to capture information. The current environment tilts the balance toward monitoring where records are handed over from running applications and routed as additional evidence and metrics. Metrics tend to be captured from more widely distributed environments. Heavier emphasis is placed on data from distributed systems and partially out of open access facilities if on-line transaction processing (OLTP) is being performed. Analytics can be performed at distributed sites and only reported when alarm situations arise. Tighter standards and alarms become possible as the time delay between events, reporting and representation decreases.

Continuous control monitoring defined

Continuous control monitoring is a management methodology aimed at facilitating corporate operations, supervision and meta-supervision through the constant measurement of corporate activity, its comparison against standards and the reporting of discrepancies leading to corrective management action. CCM puts the emphasis on controls and formalizes the control monitoring process. CCM adds focus to the role of controls in CPAS by viewing monitoring data from a control framework.

Continuous control monitoring entails audit involvement from cradle-to-grave in the design, operation and modification of corporate controls. Its main steps include:

(Continued on page 44)

- involvement in the design of corporate/system controls both of manual and computerized nature;
- involvement in the setting of standards for control and operations;
- development of a system of monitoring the operation of controls;
- development of a control function reporting system; and
- interfaces and support of the internal/external audit activity.

For control monitoring, an expanded set of systems features is desirable. These include a basic set of controls to be monitored, a series of **control reports**, a macro-schema of **control indices aggregation rules**, a schema of **control relationships** and, ultimately, a set of **control metrics** that aggregate control performance, leading to a final **control evaluation measure**.

> "The trend is to implement the whole company information system as an Intranet in which open standard technology wins."

CCM improves the quality and timeliness of corporate controls and consequently increases the efficiency of external and internal audit productivity. It adds a control overlay to the basic CPAS structure.

The advent of inter-networking and semi-universal inter-connectivity changed the scenario of corporate systems by increasing external-based exposures and providing a technology of packet-based ubiquitous data processing. While the current emphasis in Intranets decreases these exposures and facilitates internal auditing, it also creates a more complex environment and a more distributed data structure.

The evolution of the concepts

The basic elements of the CPAS paradigm, as described earlier, are modified by a more **distributed** environment, **system probing** through the handing over of standardized records, the embedding of **control agents**, and **resident analytics** that are placed in cooperating network computers and fire off **alarms and messages** when conditions of imbalance are found.

In addition to the new elements introduced to continuous process auditing, the overlay concept of continuous control monitoring is also enhanced by **resident control analytics, lurking controls, and control agents** similar to the elements described.

Resident control analytics are analytics that reside on cooperating (auditee) sites that evaluate the status of particular sets of control. For example, these controls examine site accesses and identify repeat access attempts, copies of password files, etc. Site managers and auditors are informed of these events.

Lurking controls are silent controls that reside in distributed auditee sites and pass information to the control monitoring device. For example, in a bank these controls evaluate transactions for patterns of money laundering and inform the internal auditors of these events without warning site management.

Control agents[6] migrate through the network performing specific control actions. For example, upon the advent of unusual usage patterns for a particular client, query agents travel through the auditee network looking for analogous activities.

This expanded view of the world uses the earlier described principles and associates them to CCM-like control overlays, reports and analytics. (See Figure 2.)

These two enhanced views-of-the-world deal with the increased free flow of information that the Internet provides as well as the entire new tool set of the client/server paradigm introduced by these technologies. Free flow of information may enhance efficiency and effectiveness but is a security concern. The security element is described later as transactions.

Continuous on-line distance disclosure (Internet impact on corporate governance)

The trend is to implement the whole company information system as an Intranet where open standard technology wins. Greater access to company data for shareholders and financial analysts becomes possible through computer networking. Large shareholders and analysts may be connected to certain parts of company's information system (Intranet) and monitor the company's performance on a day-to-day basis. This technology can also be used for greater disclosure and may have a profound impact on corporate governance. Consequently, the trend may be toward greater voluntary disclosure leading eventually to a snowball effect where the legal concerns relative to voluntary disclosure are out-weighted by improved and finer information sets.

Risks and security of on-line information flows

The nature and the magnitude of the Internet comparative security risk

Continuous on-line auditing deals with sensitive information that requires high levels of security. Information on the Internet flows in packets that traverse the Internet hop by hop from one router ("Internet switch") to another. Different parts of the Internet infrastructure are privately owned and operated. It is therefore difficult, if not impossible, to know in advance through which routes and routers the packets will flow, and who will have access to those routers. At each router, a packet can be intercepted and related packets can be reassembled by unwanted parties to reproduce the original message.

> "This fundamental property of the Internet design is at the core of risk exposure on the Net."

This fundamental property of the Internet design is at the core of risk exposure on the Net. It explains the special attention focused on the security (e.g. confidentiality, integrity, and authentication) of the Internet information flows. Information flows include all the electronic financial transactions (payments, fund transfers). The problems of security remain the same, whether it is a password for an auditee's corporate account, credit card information or the most recent internal report to management.

While the packets of each message can travel through different routes, all of them have to pass through the same entry point to and the same exit point from the Internet. At these points (which are usually unique), all packets can be intercepted, and the original message can therefore be reassembled with relative ease. Therefore, the risk of exposure specific to the Internet is the greatest at the entry point for a message sender and at the exit point for a message recipient.

Similar interception risks exist in other transport and communication systems. Telephone messages can be easily intercepted by tapping into a line. Since typically the number of different owners of telephone circuits is relatively small compared with the number of Internet parts owners, the number of potential telephone interceptors is smaller than their Internet counterparts, and their ranks can be better controlled. Postal messages can be intercepted and read by unscrupulous postal workers and sorters. It is difficult to assess the comparative risks of interception in various transport systems. Despite all the attention the Internet security risks are now getting in the press, we are not aware of any hard evidence to the effect that such risks are any higher than the security risks in other transport and communication systems.

At the same time, the Internet potentially offers greater opportunities for automated high-volume fraud. For example, the proliferation of credit card transactions on the Internet and the openness of the network to third parties create a possibility to intercept information about names, numbers and expiration dates of a very large number (hundreds of thousands) of credit card accounts. This information can be used to forge credit cards. These forgeries can be "automated" through computer programs automatically scanning the Internet round the clock so as to carry out fraudulent procedures continuously.

Secure electronic transaction specifications by credit card companies

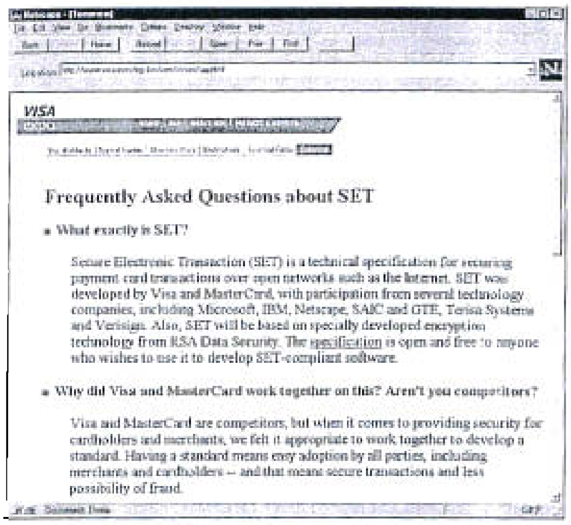
With the growth in Internet commerce, issues of security of information flows on the Net have come to the forefront of developments in Internet technology. A variety of products for securing the Internet information flows are currently available on the market. Inter-operability and a degree of standardization of these security products are needed to facilitate a faster development and wider acceptance of Internet commerce. A major milestone along these lines was the February 1996 announcement by Visa Card® and MasterCard Card® of the common specifications of secure electronic transactions (SET). See figure 3.

Both Visa and MasterCard make this specifications draft freely available on-line and solicit comments from interested parties. (See Figure 3.) According to the draft:

> *The Secure Electronic Transaction (SET) specification is divided into two separate documents: the SET business section and the SET technical specification.*
>
> *The SET business section provides an overview of the potential opportunities for bankcard associations to participate in the future growth of electronic commerce....*
>
> *The SET technical section contains the information and processing flows for SET protocol. It is intended as an introduction for anyone interested in the processing of bankcard transactions on electronic networks. It is also intended for vendors developing software that will inter-operate with other implementations of SET. The scope of the SET technical section is limited to the payment process and the security*

46)

Figure 3



Frequently Asked Questions about SET

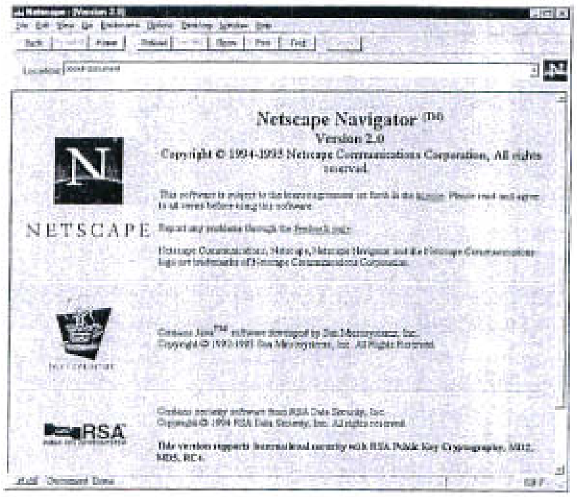
- What exactly is SET?

  Secure Electronic Transaction (SET) is a technical specification for securing payment card transactions over open networks such as the Internet. SET was developed by Visa and MasterCard, with participation from several technology companies, including Microsoft, IBM, Netscape, SAIC and GTE, Terisa Systems and Verisign. Also, SET will be based on specially developed encryption technology from RSA Data Security. The specification is open and free to anyone who wishes to use it to develop SET-compliant software.

- Why did Visa and MasterCard work together on this? Aren't you competitors?

  Visa and MasterCard are competitors, but when it comes to providing security for cardholders and merchants, we felt it appropriate to work together to develop a standard. Having a standard means easy adoption by all parties, including merchants and cardholders – and that means secure transactions and less possibility of fraud.

Figure 4



Netscape Navigator (TM)
Version 2.0
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Report any problems through the feedback page.

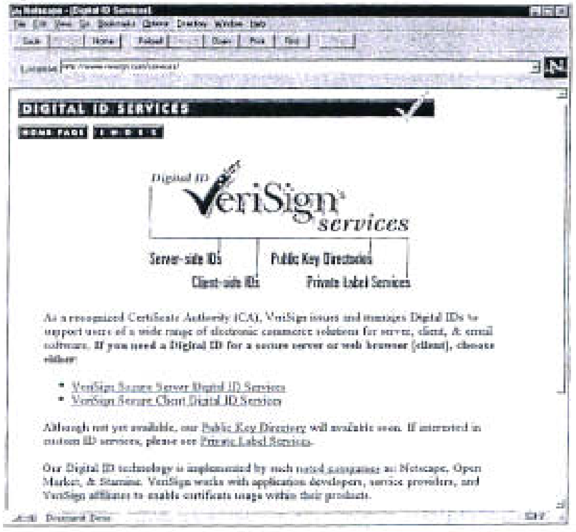
Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

Contains Java™ software developed by Sun Microsystems, Inc. Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.

Contains security software from RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. All rights reserved.

This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.

Figure 5



As a recognized Certificate Authority (CA), VeriSign issues and manages Digital IDs to support users of a wide range of electronic commerce solutions for server, client, & email software. If you need a Digital ID for a secure server or web browser (client), choose either:

- VeriSign Secure Server Digital ID Services
- VeriSign Secure Client Digital ID Services

Although not yet available, our Public Key Directory will available soon. If interested in custom ID services, please see Private Label Services.

Our Digital ID technology is implemented by such noted companies as Netscape, Open Market, & Stamina. VeriSign works with application developers, service providers, and VeriSign affiliates to enable certificate usage within their products.

services necessary to support the payment segment of electronic shopping. To provide these services, SET, in addition to defining the electronic payment protocol, also defines the certificate registration and issuance process.

Security requirements for electronic transactions

In general, there are three major security requirements in electronic commerce:

- Confidentiality of information — information should not be accessible to parties who are not authorized by the sender of that information.
- Integrity of information — information should not be alterable or lend itself to tempering with on its way from the sender to the recipient.
- Authentication of sender — the identity of the sender of information should be verifiable in a reliable manner.

Modern cryptography (the science of encryption) provides means for simultaneously satisfying these requirements. The essence of cryptography is to encrypt (cipher or code) a message in a way that the resulting coded message can be decrypted (deciphered or decoded) only by holders of the appropriate "key." In general, the term "key" refers to the password and the procedure required to decipher the encrypted message. In electronic commerce, the encryption and decryption procedures are commonly known, and the term "key" refers only to the secret "password." The password is actually a number since electronic messages are just sequences of 0s and 1s.

Cryptography is a very old science. It was traditionally based on a one key system. Both the encoder and the decoder used the same key to encrypt and to decrypt a message. As a result, the key has to be kept secret by all parties. This is why such systems are called *secret key cryptosystems*. Secret key cryptography is routinely used by the military and by the US federal government. Data Encryption Standard (DES) is a widely used secret key cryptosystem. For example, DES is used for encrypting personal identification numbers in automated teller machines. DES was endorsed as an official standard by the US government in 1977.

> *"A secret key cryptosystem cannot be used directly for electronic commerce because each merchant/customer pair will have to possess a distinct secret key."*

A secret key cryptosystem cannot be used directly for electronic commerce because each merchant/customer pair will have to possess a distinct secret key. This means that each customer should have a separate key for each merchant he or she transacts with. By the same token, each merchant should have a distinct secret key for each of his or her customers. There is therefore no feasible solution for selecting and maintaining all these distinct secret keys. Alternative cryptosystems, which made electronic commerce possible, were invented in 1976. These so-called "public key cryptosystems" are based on two keys. Each participant generates a pair of keys. One of them, the participant's *private key*, is kept secret from everybody else. The second one is the participant's *public key*, which is made publicly known. The underlying mathematics of encryption and decryption are such that if one key (either public or private) is

message, the other type of key is needed to decrypt the coded message. In other words, a message encrypted with the public key can be decrypted only using the private key. Consequently, knowledge of the public key cannot be used to decrypt a message encoded with this public key. Conversely, a message encrypted with the private key can be decrypted only using the public key. The most commonly used public key cryptosystem is RSA, invented in 1977 by Rivest, Shamir, and Adelman, and sold by RSA Data Security, Inc.

To better understand the public key cryptosystems, consider the following information exchange. Alice wishes to send a confidential message to Bob. Alice uses Bob's public key to encrypt her message. Only Bob's private key can decrypt the message. Hence, as Bob decrypts the message using his private key, he can be certain of the confidentiality of the message. But Bob cannot authenticate the fact that Alice was the one who sent the message because anyone could have used his public key and pretended to be Alice.

To enable Bob to authenticate her identity as the sender of the message, Alice has to send Bob a message encrypted with her *private* key. Now everybody can decrypt this message because Alice's *public* key is known to everyone, and everyone, including Bob, can ascertain that Alice was the sender of the message. Hence, the authenticity of this message is established because only Alice knows her private key.

In theory, to assure Bob that her message is confidential and authentic Alice has to send a message encrypted twice. Alice first encrypts her message with her private key, and subsequently encodes the encrypted message with Bob's public key. This way, only Bob can decrypt the resulting message (assuring its confidentiality), which only Alice could have sent (assuring its authenticity).

In practice, this procedure is not used often because of the very poor computational performance of public key cryptosystems. The old secret key cryptosystems are about a hundred times faster (!) than public key cryptosystems. As a result, a practical hybrid procedure combining the two techniques has been developed to secure on-line information flows.

To assure confidentiality of the message, Alice (the sender) generates randomly a secret key, and subsequently uses this random secret key to encode her message. She then uses Bob's public key to encrypt the random secret key, and sends this encoded secret key together with the encoded message to Bob. At his end, Bob first uses his private key to decode the random secret key, and then uses this secret key to decode the message. Confidentiality is assured because nobody except Bob knows Bob's public key, and the chances of randomly generating the same secret key are negligible.

To assure integrity and authentication of her message to Bob, Alice adds a so-called "digital signature" to her message. This digital signature is designed to provide irrefutable proof that the message was not altered and was signed by Alice. Digital signatures are based on a procedure of "message digesting" which message (of any length). Several different messages may have the same digest, but it is extremely difficult to produce any of them from the digest. Even the slightest change in the message generates major changes in the digest. Consequently, a message cannot be altered without significantly affecting the digest. Therefore a digest can guarantee the integrity of a message if it is appropriately protected (otherwise, a fraudulent message can be fabricated together with its digest).

To complete the procedure, Alice encodes the digest of the message with her private key, and then sends her message to Bob together with its encrypted digest. This encrypted digest is Alice's digital signature. When Bob receives Alice's message, he uses her public key to decrypt the digest. Subsequently, Bob runs the same message digest algorithm on Alice's message to obtain its digest independently and to check that this digest coincides with the digest that arrived with Alice's message. If the two digests coincide, Bob can be sure that the message is not altered (proving integrity) and is authored by Alice (providing authentication).

> *"Continuous Control Monitoring (CCM) improves the quality and timeliness of corporate controls and consequently increases the efficiency of external and internal audit (productivity)."*

Messages can be authenticated but not confidential, or confidential but not authenticated. To achieve *both* confidentiality and integrity with authentication, Alice should first create her digital signature for the message, then encrypt the resulting authenticated message with a random secret key and, ultimately, encrypt the secret key with Bob's public key.

For illustration purposes, consider how these techniques are employed in securing communications over the Internet. When Alice surfs the Internet using a secure Web browser (e.g. Netscape or Internet Explorer) and wants to communicate with a secure Web site run by Bob using a secure Web server (e.g. Netscape Commerce Server), Alice's browser will first obtain Bob's server public key. The browser then generates a random secret key, encodes it with the server's public key and sends it to the server. After the server decodes it using its private key, both the browser and the server know the secret key and can communicate confidentially by encoding their messages. The cryptographic algorithms used by Netscape can be seen in its "Help | About Netscape..." screen. RSA is a public key cryptosystem, RC4 is a secret key cryptosystem, MD2 and MD5 are message digest algorithms. (See bottom of Figure 4.)

Note that all the aforementioned procedures are publicly known. Only the secret keys and the private keys are unknown. Also, there are no mathematical proofs of the relative difficulties in deciphering these procedures. It is however universally believed that they are extremely difficult if not impossible to break. The longer the key, the more difficult it is to break the code. Moreover, linear growth in the key size leads to exponential growth in the difficulty of breaking the code. As

(Continued on page 48)

faster computers permit longer keys, advances in hardware make these cryptographic procedures more difficult to break.

How secure should on-line systems be? Faster computers can handle longer keys, thereby providing more security. From a cost-benefit viewpoint, it is possible to over-secure a system. There is clearly an optimal level of security. The key should be long enough to make the cost of breaking the code exceed the benefits. It should not be much longer than that if excessive costs associated with the cryptographic systems (e.g. hardware and software costs) are to be avoided.

There remains the problem of verifying the identity behind a public key. Who guards the guards? How can Bob be sure that Alice's public key really belongs to Alice rather than to an impostor who claims to be Alice. One solution is to have trusted authorities (called certificate authorities) whose public keys are publicly known and trustworthy. Any party can request (or buy) a digital certificate from a certificate authority, e.g. this party's public key digitally signed by this certificate authority. If Bob receives a digitally signed message from Alice together with Alice's digital certificate, Bob then can use the certificate authority's public key to extract Alice's public key from her certificate and be sure that it belongs to Alice.

> *"...the Internet potentially offers greater opportunities for automated high volume fraud."*

VeriSign, Inc. <http://www.verisign.com/> is in the business of providing digital authentication services and products for electronic commerce and other forms of secure communications. The company was founded in 1995 as a spin-off of RSA Data Security. Its investors and partners currently include Ameritech, Visa International, Netscape, Open Market and IBM.

Security of on-line sites

The best efforts to secure information flows on the Internet will come to naught if the end points are vulnerable. To that end, tight security of on-line sites has to be established. The following quote from the Computer Emergency Response Team (CERT) Web site illustrates this issue: "From January through December 1995, the CERT Coordination Center received 32,084 e-mail messages and 3,428 hotline calls. We handled 2,412 computer security incidents during this period. More than 12,000 sites were affected by these incidents, which involved 732 break-ins and nearly that many probes and pranks." An important role of internal auditors is to participate in developing a comprehensive Internet security policy for the corporate site. The auditor should review the design and implementation of the system including firewalls. For more information, auditors can review the following Web sites: <http://www.cert.org/cert.report.95.html> or <www.sei.cmu.edu/SEI/programs/cert>.[6]

Concluding remarks

The evolution of the Internet is opening many opportunities and concerns for auditors. Two major opportunities are the facilitation of continuous control and monitoring possibilities and the potential for increased and multi-layered reporting. Continuous auditing will tend to be initially implemented in highly material situations and sensitive environments. Sensitive environments make security concerns paramount.

Cryptographic technology is at the core of securing information flow on the Internet. This technology provides means of satisfying the requirements of confidentiality, integrity and authentication of electronic transactions.

Author's note: for more information, refer to the Visa Card home page at:
<http://www.visa.com/cgi-bin/vee/sf/set/intro.html>.

Endnotes

[1] Vasarhelyi, M. A. & Halper, F. B. (1992) The Continuous Process Audit System: Knowledge Engineering and Representation. *EDPACS*, 1992.

[2] Vasarhelyi, M. A. & Halper, F. B. (1991) The Continuous Process Audit System: A UNIX-Based Auditing Tool, The EDP Auditor Journal (1) 1991.

[3] Vasarhelyi, M. A. & Halper, F. B. (1991) Continuous Process Auditing in *Auditing: A Journal Of Practice and Theory*. Fall 1991.

[4] Vasarhelyi, M. A. & Halper, F. B. (1991). UNIX and Auditing. *The EDP Auditor Journal* (III) 1991.

[5] Vasarhelyi, M. A. & Halper, F. B.(1996) *Continuous Control Monitoring: A Monograph*. Submitted to the Institute of Internal Auditors.

[6] (1994) Conversations with Marvin Minsky about agents. *Communications of the ACM* (37) 7, pp. 23-29.

[7] Cobb, Stephen (1996). Firefighter, Lumberjack, Auditor. *IS Audit & Control Journal* (1) 1996, 36-39.

Alexander Kogan, Ph.D.
received his bachelor's and master's degrees in operations research from Phystech–Moscow Institute of Physics and Technology, and his Ph.D. in computer science from the USSR Academy of Sciences. With his research efforts centered on expert systems and artificial intelligence and accounting information systems, Alex has published over 20 papers. He currently is assistant professor of accounting and IS for Rutgers University and Webmaster of the RAW.

Ephraim F. Sudit, Ph.D., M.B.A.
is professor of accounting and IS at Rutgers Graduate School of Management, director of Rutgers MBA program in professional accounting and associate director of the Rutgers Accounting Research Center. Published in professional journals on the subjects of productivity, cost and quality management, Frank is the author of Productivity-Based Management and the soon-to-be-released Effectiveness Quality and Efficiency: A Management Approach.

Miklos A. Vasarhelyi, Ph.D.
is KPMG Peat Marwick professor of accounting at Rutgers Graduate School of Accounting and consulting technical manager for the advanced computing group at AT&T Bell Laboratories. His research interests focus on continuous control monitoring, Internet, economics of telecommunication and intelligent databases. Miklos is the director of the Rutgers Accounting Research Center.