UNIT-IV

Electronic Payment Systems: Special features required in payment systems, Types of E-payment systems, E-Cash, E-cheque, credit card, Smart Card, Electronic Purses, E-Marketing, E-Customer Relationship Management, E Supply Chain Management.

Security Issues in E-Commerce: Security risk of E-Commerce, Types of threats, Security tools and risk management approach. Cyber laws, Business Ethics.

15

Type of Electronic Payment Systems

ELECTRONIC PAYMENT SYSTEMS

The concept of electronic commerce relates to selling goods or services over the Internet. This involves making payments over the Internet. Thus *on-line pay-ment systems and E-commerce are intricately linked given that on-line consum-ers must pay for products and services which they are using online.*

Electronic payment systems are proliferating in banking, retail, health care, Gems & Jewellery, Handicraft, Fashion, garments, on-line markets and even government, infact, anywhere money needs to change hands. Organizations are motivated to use electronic payment systems by the need to deliver products and services more *cost effectively* and to *provide higher quality of service to the customers.* Customers are encouraged to use the electronic payment systems because of the ease of mak-ing payments through them.

Research into electronic payment systems can be traced back to 1940s when the first applications-the credit cards-appeared. In 1 970s, the emerging electronic payment technology was labelled as electronic funds transfer (EFT). EFT is defined as "any transfer of funds initiated through an electronic terminal, telephonic instru-ment or computer or magnetic tape so as to order, instruct or authorise a financial institution to debit or credit an amount". EFT uses *computer and telecommunica-tion* components both to supply and to transfer money or financial assets. *Transfer is information based and intangible.* Thus EFT sands in marked contrast to con-ventional money and payment modes that rely on physical delivery of cash or cheques. The EFT or electronic payment system may mean differently to consumers, suppli-ers of goods, banks or financial institutions, corporate house, organization etc.

To a consumer, an electronic payment system is a convenient way of making a purchase or paying for a service without having to hold physical cash or going

through the process of completing a cheque. This may be achieved through a credit card, on-line or off-line, electronic cash, electronic cheque, smart card etc, which are termed as Electronic Money.

Electronic money (also known as electronic cash, electronic currency, digital money, digital cash or digital currency) refers to money or scrip which is exchanged only electronically. Typically, this involves use of computer networks, the internet and digital stored value systems. EFT and direct deposit are examples of electronic money. Also, it is a collective term for financial cryptography and technologies enabling it.

To a supplier of goods or services an electronic payment is the receipt or out-ward movement of funds, which may be from consumers as bill payments, outgoing payments to suppliers for materials or to employers as salary payments. Such elec-tronic payment systems may be linked into an inventory management or accounting system, eliminating the time-consuming clerical activities and offering easier man-agement of cash flows. To a bank or financial institution, an electronic payment is a series of processes by which value exchange is captured, verified and accepted, a series of checks, balances and reconciliation's to ensure integrity. Such electronic payments are always in conjunction with a series of accounting entries. Electronic payment systems need to fulfill *certain requirements* in order to emulate the properties of the existing payment schemes. Some of these requirements are:

- **Acceptability:** Payment system needs to be widely acceptable in order to be successful.
- **Convertibility:** It should be able to be converted into into other types of funds.
- **Efficiency:** The cost per transaction should be very low or nearly zero.
- **Flexibility:** Several methods of payment should be supported.
- **Reliability:** The payment system needs to be highly reliable.
- **Scalability:** Allowing new customers and suppliers into the system should not break down the infrastructure.
- **User Friendly:** Payment should be as easy as in the real world.
- **Security:** Electronic payment systems should allow financial transactions over open networks, such as the Internet.

Conventional Payment Process

A conventional process of payment and settlement involves a buyer-to-seller transfer of cash or payment information (e.g. credit card or check). The actual settle-ment of payment takes place in the financial processing network. A cash payment requires a buyer's withdrawal from his bank account, a transfer of

cash to the seller, and the seller's deposit of the payment to his account. Non-cash payment mecha-nisms are settled by adjusting, i.e. crediting and debiting, the appropriate accounts between the banks based on payment information conveyed via check or credit card. Figure below is a simplified diagram for both cash and non-cash transactions. Cash moves from the buyer's bank to the seller's bank through face-to-face exchanges in the market. If a buyer uses a non-cash method of payment, payment information instead of cash flows from the buyer to the seller, and ultimately payments are settled between affected banks who notationally adjust accounts based on the payment in-formation. In real markets, this clearing process involves some type of intermediaries such as credit card services or check clearing companies. Schematically then most payment systems are based on similar processes. The 'information' conveyed to settle payments can be one of the following :

- information about the identities of the seller and the buyer and some instruction to settle payments without revealing financial information
- financial information such as credit card or bank accounts numbers (including checks and debit cards)
- actual values represented by digital currency

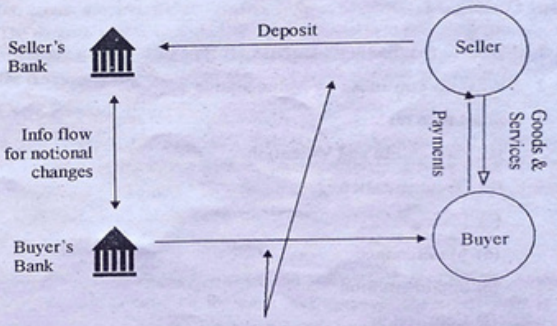


Figure 15.1 : A simplified model of transaction

Types of Electronic Payment Systems

Electronic commerce, especially that involving consumers and digital products, places stringent demands on a payment system. Electronic commerce payment systems must be convenient for Web purchasing, transportable over the network, strong enough to thwart electronic interference, and cost effective for

extremely low value transactions. Despite this impressive set of requirements, there have been over two dozens proposed Internet payment standards or protocols. These range from Anony-mous Internet Mercantile Protocols by AT&T Bell Labs to Conditional Access for Europe (CAFE.) for the European community, to Secure Electronic Transaction (SET) promoted by MasterCard. Many software and hardware products based on these open standards are being offered, including CyberCash, Digicash, Mondex, NetBill and NetCheque. While the diversity of these products is an indication of healthy competition, it does make it confusing for ordinary Internet users and merchants to choose an appropriate payment mechanism. To structure the following discussion of types, we suggest all electronic payment systems can be broadly classified into three groups:

- Payment through an intermediary,
- Payment based on EFT
- Payment based on electronic currency.

Payment Through an Intermediary—Payment Clearing Services

When iaifc-to-face purchase is replaced with on-line commerce, many aspects of a transaction occur instantly, under which various processes of a normal business interaction are subsumed. For example, a typical purchase involves stages of locating a seller, selecting a product, asking a price quote, making an offer, agreeing over payment mt-ans, checking the identity and validity of the payment mechanism, trans-ferring of goods and receipts. In order to be used as a substitute for face-to-face payments, online payment systems must incorporate all or some of these stages within their payment functions.

The lack of face-to-face interaction also leads to more secure methods of pay-ment being developed for electronic commerce, to deal with the security problems to! sensitive information and uncertainty about identity. Consequently, electronic com-merce transactions require intermediaries to provide security, identification, and au-thentication as well as payment support.

Figure below shows a stylized transaction for online commerce using an inter-mediary. In this model, the intermediary not only settles payments, it also takes care of such needs as confirming seller and buyer identities, authenticating and verifying order ing and payment information and other transactional requirements lacking in virtual interactions. In the figure, two boxes delineate online purchasing and secure or off-line payment clearing processes. Payment settlement in this figure follows the example of the traditional electronic funds transfer model which uses secured private value networks. The intermediary contributes to market efficiency by resolving un-certainties about security and identity and relieving vendors of the need to set up duplicative hardware and software to handle the online payment clearing process.

The payment information transmitted by the buyer may be one of threv-lypes. First, it may contain only customer order information such as the identity of the buyer and seller, name of the product, amount of payment, and other sale conditions but no payment information such as credit card numbers or checking account numbers. In this case, the intermediary acts as a centralized commerce enabler maintaining mem-bership and payment information for both sellers and buyers. A buyer need only send the se! ler his identification number assigned by the intermediary. Upon receiving the purchase order, the intermediary verifies it with both the buyer and seller and handles all sensitive payment information on behalf of both. This is the electronic commerce model followed by First Virtual Holdings

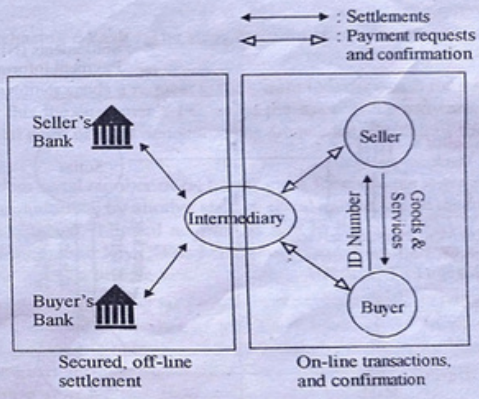


Figure 15.2 : Transactions with an intermediary

The key benefit of this payment clearing system is that it separates sensitive and nonsensitive information and only non-sensitive information is exchanged online. This alleviates the concern with security that is often seen as a serious barrier to online commerce. In fact, First Virtual does not even rely on encryption for messages between buyers and sellers. A critical requisite for this system to work is the users' trust in the intermediaries.

Payment Based on EFT—Notational Funds Transfer

The second type of payment systems does not depend on a central processing intermediary. Instead, sensitive payment information (such as credit card or bank account number) is transmitted along with orders, which is in effect an open Internet implementation of Financial Electronic Data Interchange (EDI). An Electronic Funds

Transfer (EFT) is a financial application of EDI, which sends credit card numbers or electronic checks via secured private networks between banks and major corpora-tions. To use EFTs to clear payments and settle accounts, an online payment service will need to add capabilities to process orders, accounts and receipts. In its simplest form, payment systems may use digital checks —simply an image of a check— and rely on existing payment clearing networks. The Secure Electronic Transaction (SET) protocol—a credit card based system supported by Visa and MasterCard—uses digital certificates, which are digital credit cards. We call this type of payment system as notational funds transfer system since it resembles traditional electronic fund trans-fers and wire transfers which settle notational accounts of buyers and sellers.

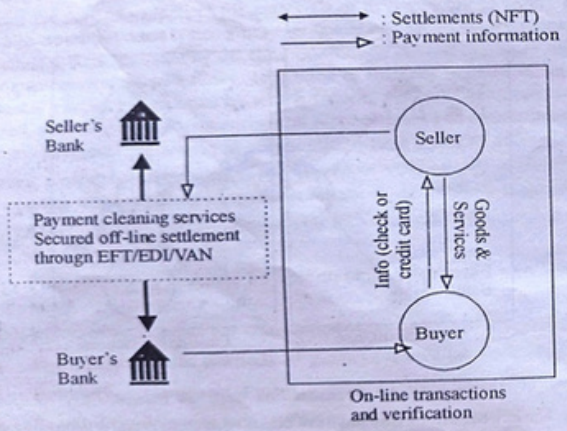


Figure 15.3 : Notational funds transfer system

Notational funds transfer systems differ from payment clearing services in that the 'payment information' transferred online contains sensitive financial information. Thus, if it is intercepted by a third party, it may be abused like stolen credit cards or debit cards. A majority of proposed electronic payment systems fall into this second type of payment systems. The objective of these systems is to extend the benefit and convenience of EFT to consumers and small businesses. However, unlike EFTs, the Internet is open and not as secure as private value added networks (VANs). The challenge to these systems is how to secure the

integrity of the payment messages being transmitted and to ensure the interoperability between different sets of payment protocols.

Payment Based on Electronic Currency

The third type of payment systems transmit not payment information but a digital product representing values: electronic currency. The nature of digital currency mirrors that of paper money as a means of payment. As such, digital currency payment systems have the same advantages as paper currency payment, namely anonymity and convenience. As in other electronic payment systems, here too security during transmission and storage is a concern, although from a different perspective, for digital currency systems doublespending, counterfeiting, and storage become critical issues whereas eavesdropping and the issue of liability (when charges are made without authorization) are important for notational funds transfers. Figure below shows a digital currency payment scheme.

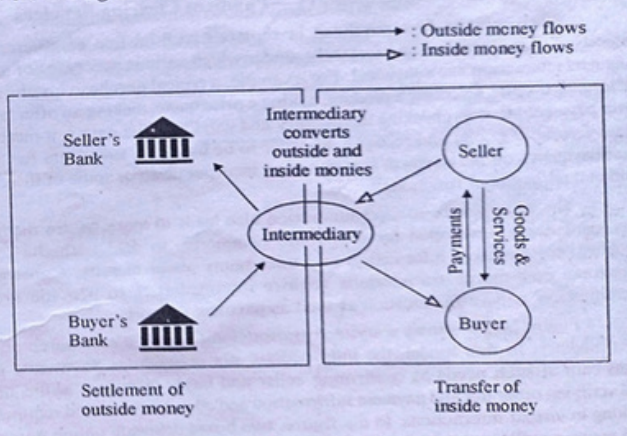


Figure 15.4 : Digital currency payment system

The only difference from Figure is that the intermediary in Figure above acts as an electronic bank which converts outside money (e.g. U.S. currency), into inside money (e.g. tokens or e-cash) which is circulated within online markets. However, as a private monetary system, digital currency will have wide ranging impact on money and monetary system with implications extending far beyond mere transactional efficiency. Already digital currency has spawned many types of new businesses: software vendors for currency server systems; hardware vendors

for smart card readers and other interface devices; technology firms for security, encryption and authentication; and new banking services interfacing accounts in digital currency and conventional currency, e.g. Mark Twain Bank. Many of these new players navigate through areas uncharted by researchers and government policy makers. Old maps used to inscribe unknown territories with "Here Be Dragons," a cartographic term for uncertainty. What kinds of dangerous as well as fascinating "dragons" we will encounter in this new world of electronic payments is the subject of the remaining sections.

CYBER CASH / ELECTRONIC CASH

Cyber Cash, Electronic cash, e-cash, *digital money* or *digital cash* provides the means to transfer money between transacting parties over a network such as the Internet. Electronic cash must satisfy some general properties of digital money.

1. Monetary Value: E-cash must have a monetary value *i.e.* it must be **backed either by cash** or bank authorized credit.

2. Interoperability: E-cash must be interoperable *i.e.* exchangeable as pay-ment for other e-cash, paper cash, goods or services, credit, deposits in banking accounts and the like. Also e-cash should be interoperable between multiple banks and be- tween multiple currencies.

3. Security: E-cash should not be **easy to copy orjduplicate.** A tricky issue in. the use of e-cash is 8-*spending.* For instance, one could use the same e-cash to buy some- thing in Japan, India and England simultaneously. Preventing double spending from occurring is extremely difficult. For this reason, most systems rely on post- fact detection and punishment.

4. Diversibility: E-cash must be available in **several denominations.** It should also be divisible a way similar to real cash.-

Electronic Cash System

Electronic cash is based on *cryptographic systems called "digital signatures ".* This method involves a pair *of numeric keys* that work in tandem: *one for locking (or encoding) and the other for unlocking (or decoding).* Messages encoded with one numeric key can only be decoded with the other numeric key and none other. *The encoding key is kept private and the decoding key is made public.*

By supplying all customers (buyers and sellers) with its public key, a bank en-ables the customers to decode any message (or currency) encoded with the private key. If decoding by a customer yields a recognizable message, the customer can be fairly confident that only the bank could have encoded it. These digital signatures are very secure and have proved to be more resistant to forgery than handwritten signstures. *Before e-cash can be used to buy products or services,*

it must be pro-cured from a currency server. In e-cash technology such an electronic cash issuing server is called the *e-mint.* The e-mint issues the electronic cash based on the funds provided by the customer in various denominations. The customer can use this e-cash to purchase items over the internet.

Any party involved in an e-cash transaction must necessarily maintain an ac-count with an e-mint. The *Deutsche Bank, The Mark Twain Bank and the St. George s Bank in Australia* are some of the Banks offering e-cash services.

The electronic cash transactions take place in three distinct and independent phases.

I. Purchasing e-cash : The steps involved in the purchase of e-cash from an e-mint are:

The customer sends a request to the e-mint to issue e-cash for some amount of money. For this the customer's PC, using the appropriate software, calculates how many digital coins of what denominations are needed to withdraw the requested amount.

A random serial number of 64 bits or more for each coin is generated. This serial number is multiplied by another random serial number cai'ed the *blmdingfac-tor* and the so obtained "blinded number" is sent to the e-mint server encrypted: using the banking public key. "The bank or e-mint server decrypts the encoded blinded number using its private key.

The e-mint server using its private key creates a digital signature, or blind signature from the blinded number or token and sends it back to the customer's computer. The customer is able to divide the blinded number by the blinding factor and get the original serial number back. *The original serial number plus the digital signature sent by the bank are the digital coins., their value being guaranteed by the bank.* A customer may store the digital coins on his hard drive or smart card. In exchange of the e-cash money is debited from the customer's account.

II Purchasing with Electronic Cash : A customer may use e-cash to purchase products or services on-line.

- The customer selects the goods or services and transfers the digital coins to the merchant.
- The merchant provides the goods to the customer.

III. Redeeming Cash by the Merchant: The merchant transfers the e-cash to the e-mint.

- The e-mint credits the merchant's account with the money.

The above example shows the exchange of electronic cash between a customer and seller. Similar transfer of e-cash may take place between two

individuals or institutions such as banks, universities or other businesses. Now we will discuss in detail that how Electronic cash payment process actually works.

How Cyber Cash Payment Works

Cyber Cash transactions are completed between three separate software programs: one program that resides on the consumer's PC (Cyber Cash Wallet), one that operates as part of the merchant server, and one that operates within the Cyber Cash servers. Before shopping with Cyber Cash, consumers download Cyber Cash Wallet program which is available freely from Cyber Cash Since the Cyber Cash Wallet is a separate piece of software, consumers can use any type of credit card. A Cyber Cash payment process, depicted in Figure below, works in the following manner:

(1) The consumer selects items for purchase and fills out the merchant's order form, complete with necessary shipping information.

(2) When the shopper selects to pay with Cyber Cash, the merchant server presents an invoice to the consumer and requests payment, sending a special message to the consumer's Cyber Cash Wallet. The consumer simply chooses which credit card to pay with and clicks on it.

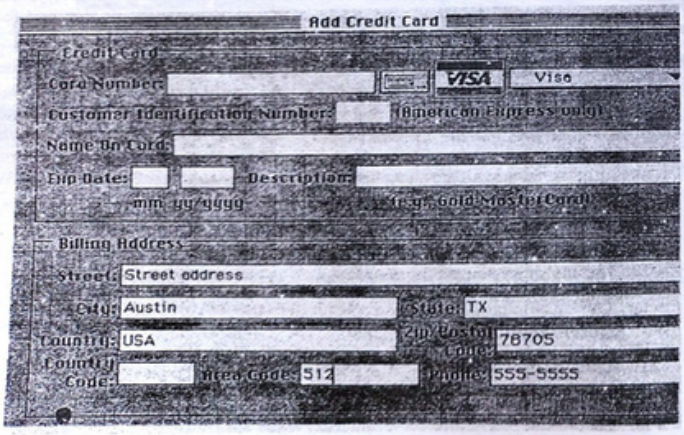


Figure 15.5 : Cyber Cash Wallet keeps user's credit card information

(3) Cyber Cash Wallet sends credit card information to the merchant server.

(4) The merchant server verifies the validity and integrity—that is to check whether or not it was tampered with—of received message, and sends it to a CyberCash server,

(5) CyberCash server is linked to a credit card payment network, where accounts are settled by conventional processes.

(6) Payment settlement result is forwarded to the CyberCash server.

(7) Merchant server is notified of the transaction result.

(8) Merchant sends ordered items with receipt to the shopper.

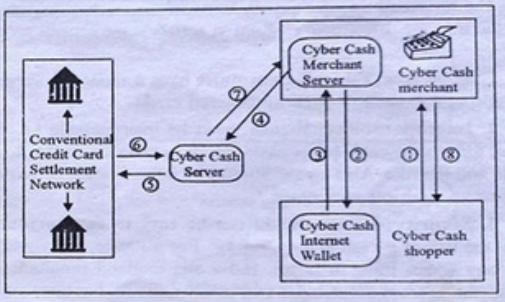


Figure 15.6 : Cyber Cos/i payment clearing process

Electronic cash is *secure* as neither the customer or payei nor the merchant or payeean counterfeit the bank's digital signar.lfe. The payer and the payee can verify that the payment is valid, since each knows the bank's public key and only the bank's private key could have generated the digital signature.

Electronic cash can be completely *anonymous*. Anonymity allows freedom of usage- buy illegal or legal products and services. This is accomplished in the following manner. When the e -cash software at the customer end generates a random serial lumber, it marks or blinds the original number using a blinding factor and sending it to he bank. The "blinding" carried out by the customer's software makes it impossible or anyone to link the payment to the payer. Even the bank cannot connect a digital :oin to a customer, since the customer's original token was blinded when it was signed by the bank or e-rnint. Thus the e-cash system creates anonymous, untraceable currency.

A problem associated with e-casH is that of *double spending*. However to uncover double spending, the bank or e-mint must compare the digital coin passed

to it for redemption against a database of spent coins. However the method of matching digital coins with a central database has problems of *cost overheads, especially where the denominations are very small.*

A drawback *oi* e-cash is its *inability to be easily divided into smaller amounts.* It is often iccessary to get small denomination change in busiriess transactions.

The *enormous currency fluctuations* in international finance pose another problem and the event of sudden devaluation of certain currency-whc holds the iiability-the buyer or the seller? For such obstacles, e-cash in its early forms may be denominated in single currencies and exchanged at conventional market rates. There are also operational risks associated with e-cash and these may be mitigated by imposing constraints such as limits on-

1. The Time over Which a Given Electronic Money is Valid. Time limits could be set beyond which the electronic money would expire and become worthless. The customer would have to redeem or exchange the money pi ior tc the expiration deadline. For this feature to work, electronic money would have to be time stamped,
2. How much can be Stored on and Transferred by Electronic Money. A maximum upper limit could be imposed on the value that would be assigned to any single transaction or that would be transferred to the same vendor within a given period of time.
3. The Number of Exchanges that can lake Place Before a Money Needs to be Redeposited With a Bank. A ceiling could be imposed on the number of exchanges that would be permitted before any electronic money would have to be redeposiled in a bank and reissued.

The above constraints introduce a whole new set of implementation issues and involve overheads. Considering the relative benefits and limitations of e-cash. it is not very clear vet that the market as a whole will adopt an anonymous e-cash standard. For now, e-cash is only a likely path 10 may fuuire h-jsiness transactions. How well it succeeds is to be seen.

Properties and Specifications of Digital Currencies

Digital currencies are digitally exchangeable cash. Therefore, digital currencies and payment systems rrmst satisfy both the monefarv properties expected of cash arid the requirements of' .he digital communication network If is actually a rather simple matter to extend the NFT model into a value transfer model where actual monetary value is exchanged, similar to any type of currency, instead of account information. CyberCash discussed as an NFT system is in fact implementing an extension of its system to enable peer-to-pccr transactions that do not involve a TTP for authentication.

Desirable Properties of Digital Currency

Developers of digital currency have a wide range of options to implement strong safety requirements of transmitting values over the network. For example, a secure digital currency can be implemented by using strong encryption algorithms, by employing tamper-resistant hardware, or by securing the network communication. Although physical specifications of digital coins and tokens may vary, the following properties are fundamental to any digital currency payment system.

Monetary Value To be used as a monetary unit, digital currency must have value that can be exchanged for other goods and services, be used to pay fiduciary obligations, or be transferred to another person. Since digital currency is essentially a file, it does not have an intrinsic value, but must be linked to other system of value. The most common implementation is to base the value of digital currency on bank deposits, credits, or prepayments using outside money. Once a digital currency is convertible to dollars, the next step is for it to be accepted in the market as a monetary token. Once accepted and trusted, a digital currency can establish related properties such as exchangeability and transferability.

Convenience Convenience has been the biggest factor in the growth of notational currencies such as checks, which are scalable and easy to transport. Similarly, digital currencies must be convenient to use, store, access, and transport. As a digital file, it may allow remote access to money via telephone, modeiri, or Internet connection. Electronic storage and transfer devices or network capabilities will be needed. To gain wide acceptance, digital cash also must be convenient in terms of scalability and interoperability so that users need not carry multiple denominations or multiple versions for each operating system.

Security To secure physical money and coins, one needs to store them in wallets, safes or other private places If digital currencies are stored in hard drives connected to an open network, theoretically anybody can snoop and tamper with the money. Encryption is used to protect digital currency against tampering. Some proposals using smart cards, e.g. Mondex, store digital currency in tamper-resistant hardware that can be maintained offline. Ecash relies on the security of Ecach client software residing on users' computers. At the same time, digital currencies must be resistant to accidents by owners. Dollar bills are printed on strong paper that withstands many adverse treatments, such as washing. To achieve similar security, adequate protection standards are needed both in physical specifications of digital coins and in policy matters for legal and commercial liabilities.

Authentication Authentication of money is done by visually inspecting bills and coins. Although further tests could weighing, chemical analysis, and contacting the authorities, authentication is usually a simple matter for physical currency. Digital currency, however, cannot be visually inspected and it is difficult to distinguish the original and a counterfeit. Because of this, inspection of digital

currency depends on authenticating secondary information that accompanies the bills or coins such as the digital signatures of banks or payers attached to the currency (serial number). A more rigid system will require contacting a third party each time a transaction is made. Although this system is more secure, the transaction costs may be too high for small-value purchases. A hardware based system like Mondex relies on software and hardware and does not require authentication for each transfer of values. Other systems will have to strengthen their client software or introduce hardware protection to allow peer-to-peer transactions.

Non-refutability Acknowledging payment and receipt is a basic property required of a payment system. In cash transactions, simple receipt is enough to establish nonrefutability. A similar exchange of digital receipts can be used for digital transactions. An alternative is to append all transaction records into the digital currency itself. In this system, digital coins accumulate information about all parties involved in past transactions. These are called identified tokens compared to anonymous tokens, which do not reveal information about users.

Accessibility and Reliability One advantage of digital currency over cash is its capability to be transported over the network. Therefore, users can store digital money at home but access it remotely via telephone or modem, the same network used to clear payments. Because of this crucial role, digital payment systems must provide continuous, fast, and reliable connections.

Anonymity Unlike checks and cards, cash transactions are anonymous. An anonymous payment system is needed to protect against revealing purchase patterns and other consumer information, although untraceable transactions are opposed by the government in view of possible criminal uses. Nevertheless, the need will persist, and anonymity is perhaps the single most important property of cash transactions. Digital currency can be equipped with varying degree of anonymity masking the user identity to the bank, the payee, or both. Strong anonymity guarantees untraceability while a weaker version allows the user's identity to be traced when the need arises. While the issue of anonymity invokes debates about tax evasion, money laundering and other criminal uses of digital currency, the economic rationale for simple, anonymous digital coins is that they reduce transaction costs by eliminating third parties and protect consumer information that could be used to price-discriminate among consumers.

Technical Specifications of Digital Currencies

Two types of digital currency have been developed but the general trend appears to be toward a mixed system. Ecash, developed by DigiCash is the forerunner of Internet payment systems based on online transactions. Mondex represents the other type of payment system based on off-line transactions. Unlike their on-line counterparts aimed at Internet users, off-line payment systems grew out of existing electronic funds transfer mechanisms using debit cards such as telephone and copy

cards. These cards hold pre- paid account information and merchants who accept these cards are usually credited for the transaction amounts by the card issuer. By using computer chips embedded in these cards, hence the name smart cards, both payment information and values can be transferred. As issuers develop network interface devices, smart cards can be used online as well, competing directly with online payment systems. Similarly, Ecash and other online payment systems are introducing electronic wallets similar to smart cards enabling off-line transactions. As the two become integrated, the distinction between online and off-line systems is rapidly disappearing. Below, we discuss E-cash and Mondex in more detail.

E-cash : E-cash is a digital currency protocol developed by DigiCash and tested extensively on the Internet. Ecash uses public key encryption technologies to maintain the integrity of digital coins. By varying the encryption, Ecash can have strong or weak anonymity. DigiCash licenses Ecash technologies to banks, who convert outside money into digital currency and serve as currency servers in authenticating, clearing and settlement of accounts. Mark Twain Bank of St. Louis shown in Figure below, is the first electronic bank to license the Ecash technology that serves interface functions between dollar-denominated accounts and E-cash accounts.

Electronic Check

In today's competitive merchant landscape, it is vital to take advantage of emerging technologies to improve business efficiency. Electronic check processing can make accepting checks easier, safer, and more cost-effective for merchants. Benefits can include improved cash flow, minimizing losses from returned checks, lowered administrative costs, and reduced depository bank fees. Electronic check processing also can help streamline the check acceptance process, reduce paperwork, and expedite closing, balancing and settlement.

Introduction

The check payments industry is undergoing a major change, driven by significant technological advances in electronic check processing options and growing merchant demand for these solutions. Because traditional check processing methods are expensive, labor-intensive, and increasingly subject to fraud, the question for merchants today has shifted from "Should I consider an electronic check method?" to "Which electronic check method should I choose?"

Although the slow but steady decline in check payments is well documented, checks still comprise a significant portion of merchant transactions. Recent First Data/TeleCheck research indicates that within the American population, a core base of check writers exist for whom checks are the preferred method of,-payment 1. Merchants cannot afford to lose business by refusing to accept checks, but instead must make checks as effective and efficient as possible.

As electronic check processing evolves, merchants are faced with increasingly complex choices. This paper aims to help merchants analyze their options quickly, clearly and efficiently, in order to make the right decision for their specific business needs. The environments addressed by this paper generally have the following characteristics:

- Checks are currently settled in a traditional manner entailing the physical transportation of paper checks to a local bank
- Transactions consist of payment for the exchange of goods and services in a face-to-face environment
- The vast majority of checks presented are consumer checks
- Some checks are returned due to insufficient funds and fraud

Although many aspects of this paper apply to smaller merchants, it also takes into consideration larger, multi-location national and regional chains whose customers are primarily consumers (not other businesses).

Lifecycle of a Check

Check processing is composed of three interlinked sub-processes, the "ABCs".

Authorization - systems and processes that help a merchant determine whether or not to accept a check. Merchants are generally moving from static negative files to real-time verification systems based on sophisticated statistical models. Potential costs include vendor fees and lost sales on declined transactions.

Back-office/settlement - processes that facilitate the movement of funds. From a merchant perspective this process begins when a consumer hands a check to a cashier. Costs include labor, bank fees, transportation, and float costs.

Collections - processes that allow a merchant to recover funds effectively when a check is returned. Merchants have generally moved from store-based internal collections to outsourced providers of collections services. Costs include uncollected returned checks, additional bank fees and collections efforts.

Operational Characteristics

In the example shown in Figure below the business transaction begins with the payee sending an invoice or bill to the payer, which is processed by the payer's accounts payable system. When the time comes to pay the invoice, the invoice TnfoTrnation~Is retrieved from the accounts payable system, and the invoice data is used to create an echeck. The echeck includes familiar check information such as the payee's name, the amount, and the date and the account information. To sign the echeck, the payer enters a ;'!N to unlock an electronic checkbook card in the form of a smart card. Th:::; card is , secure container for the payer's private signature

key, and assures a degree of non-repudiation. The signature on the echeck may also cryptographically bind a copy ofthe invoice to the echeck, so that an attacker cannot substitute a different invoice in order to commit fraud. The invoice format is not fixed, but it can be flexible with respect to length, format and data content, so that the payer can return the document received from the payee. This provides the payee with the complete information needed to correctly post the payment.

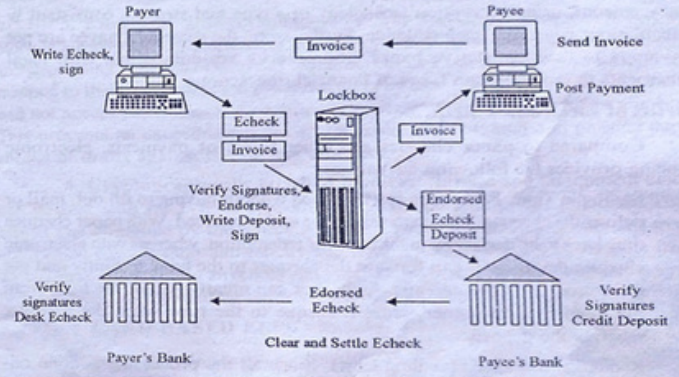


Fig. 15,7 : Electronic Check Lockbox Flow

The signed echeck and invoice is sent to the payee by email or a web transaction. The payee verifies the payer's signature on the echeck and invoice, detaches the invoice information, and posts the payment to accounts receivable. The payee enters his PIN to unlock his electronic checkbook and uses the electronic checkbook to endorse the echeck and to sign an electronic deposit slip to deposit a batch of echecks. The endorsed echeck is forwarded to the payee's bank for deposit and subsequent clearing. The clearing process can be done by integrating echeck into existing Electronic Check payment systems or other clearing and settlement systems. Both the payee's bank and payer s bank verify all signatures on the echeck and endorsement using a two layer certificate system which links the signature verification keys to the signer and signer's bank account. The paying bank verifies that this transmission of the echeck is not a duplicate, that the payer's certificate and account are currently valid, and posts the echeck to the payer's Demand Deposit Account (DDA).

Finally, the payer receives a line item on his statement, which may now carry a full description of the transaction, since the entire contents of the echeck

are machine-readable. Echecks have been designed so that the integrity, authentication and non-repudiation properties of public key signatures are sufficient to protect against fraud. Furthermore, to protect the paper check accounts against fraud, echecks use different bank account numbers, which are valid only for cryptographically signed echecks. Since encryption is not required to prevent fraud, the echeck technology is compatible with export policies regarding encryption technology. The echeck may be encrypted over any of the transmission links for privacy reasons, using encryption technology of a type and strength consistent \v it'n regulations governing each situation. Furthermore, the payer and payee are not anonymous to their respective banks, and echecks are compatible with legal requirements to report certain types of financial transactions.

Benefits of Electronic Cheques

Compared to paper cheques and other forms of payments, electronic chequeing provides the following advantages:

1. Saving in Time. F-cheques can be issued without having to fill out, mail or deliver the cheques. The processing time is also reduced. With paper cheques they have to be deposited in the bank for redemption, whereas with electronic cheques the receiver can forward the cheques to the bank instantly and get them credited to the account. E-cheques can greatly reduce the time from the moment a consumer writes a cheque to the time when the receiver receives the deposit.
2. Reduction in Paper Handling Costs. Since all the processing is done on-line, there is a great reduction in paper work involved. Cheques are received and processed on-line. Any correspondence sending back cheques to the payers or payees is also handled on-line.
3. Reduction in Bounced Cheques. E-chequeing can be designed in such a way that the receiver can get authorisation from the sender's bank before accepting the e-cheque.

Electronic Checkbooks

A handwritten signature captures the reflexive movement of the signer's muscles and is partly a biometric characteristic of the signer. This makes it difficult for a forger to create a perfect forgery, even if the forger has a sargpie of a handwritten signature. However, a perfect forgery of a cryptographic signature can be made by anyone who has the signer's private signature key. Financial Services Technology Consortium. All rights reserved.

Therefore, it is critical to establishing an echeck system based on public key signatures that payees and banks are able to trust that payers can maintain possession and control over their private signing keys at all times. Electronic

checkbook smart cards or other cryptographic hardware are used to help ensure that signatures are made only by legitimate signers, so that check forgery is made difficult. Electronic checkbook cards also standardize and simplify key generation, distribution and use, so that a high and uniform level of trust can be established without depending on the skill and diligence of every echeck customer.

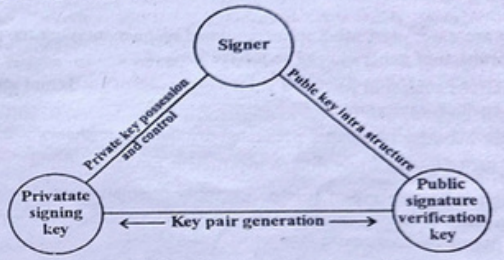


Figure 15.8 : Public Key Signature Security Fundamentals

As shown in Figure above, verifiers must believe three types of things about the signer and the signer's private and public signing keys:

1. Private key possession and control — The signature verifier must believe that the signer has exclusive possession of his signing key. If an attacker can get possession of the signer's private'key, then the attacker can forge signatures using his own system from any location on the network. If the attacker can gain control of the signer's computer, then the attacker can forge signatures without the signer's knowledge.

The electronic checkbook, in the form of a PIN-activated tamper-resistant smart card or similar cryptographic hardware, performs the signing algorithm so that the private signing key is always kept inside the trusted hardware and is never read into the signer's much more vulnerable networked personal computer or server. The electronic checkbook is aware of echeck syntax and logs critical data from echecks to provide the signer with a trusted log of signing actions.

2. Key pair generation — The signature verifier must believe that the private/ public key pair was generated such that the private key cannot be calculated or guessed by an attacker based on knowledge of the public key.

The electronic checkbook performs key generation within the tamper-resistant hardware using algorithms that have been properly tested and certified by the manufacturer. Only the public key is exported from the hardware, and the private key is never revealed to anyone.

3. Public key infrastructure — The signature verifier must be able to trust that the public key provided for use in verifying the signature really belongs to the signer and is the other half of the signer's public key pair.

The electronic checkbook is initialized using procedures based on bank card issuing processes. The public key exported from the card is included in an X.509 certificate signed by the bank's Certification Authority, and associated with an account block also signed by the bank's Certification Authority. The bank echeck servers also keep an independent database of the bank's signer's public keys, such that they always know the most current relationships of keys to accounts and signers.

Besides key management and logging functions just described, electronic checkbooks also:

1. include the checkbook's unique number (manufacturer, model and serial number) in each echeck,
2. consecutively number each echeck as it is signed, in order to ensure that each echeck is unique,
3. generate random numbers that are prefixed to blocks to increase security of the hashing functions,
4. contain signer personal data which the signer can selectively apply to echecks,
5. separately unlock echeck writing, checkbook administration and bank administration functions using PINs,
6. deactivate if PIN hacking is detected.

Furthermore, the design of the electronic checkbook must be such that the private signing key cannot be extracted via its electrical connector and any successful attempt to extract the private key will visibly damage the electronic checkbook and render it inoperable.

Fraud Prevention

A design goal of the echeck system is to prevent fraud without relying on encryption, since standard widespread availability of strong encryption has been hampered by export controls and by attempts to regulate its use. Cryptographic signature systems are quite freely used and exported, while key management and public key infrastructure components are more restricted, especially if they can also be used to manage encryption keys. Features intended to prevent fraud include:

1. Duplicate detection — Each echeck is guaranteed to be unique by the operation of the electronic checkbook. The payee and payee's bank should detect and refuse duplicate submissions of echecks, and the payer's bank must detect duplicates and pay only one instance of an echeck. This prevents multiple payments due to innocent retransmissions of email, and also prevents a payee from cashing and depositing an echeck in two different accounts.

2. Payee identification — The check block provides for checks to be made out to the payee's bank routing code and either an account or customer ID number. It also provides for an echeck to be made out to the payee's public key. These parameters uniquely identify the payee, and prevent an eavesdropper from exploiting the ambiguity of payee identification which otherwise exists if only payee common names are used. These parameters are also included in the endorsement block so that echecks can be endorsed over to uniquely identified third parties.

3. Electronic account numbers — The account number in the account block is a randomly chosen number assigned by the bank for the purpose of writing and depositing echecks. The payer's and depositor's echeck account numbers are mapped to their paper check account numbers by their respective banks. The banks will not accept paper checks or drafts written against the echeck account numbers. This prevents an eavesdropper or corrupt payee from printing and passing paper checks or drafts against the account numbers.

4. Cryptographically attached invoices - Invoice and attachment blocks can be sent with the echeck blocks to detail the purpose of the payment. These blocks can be signed by the echeck signature, which binds these documents to the echeck and ensures their authenticity and integrity. This prevents an attacker from, for example, intercepting an echeck and purchase order, changing the delivery address in the order, and forwarding the echeck and altered order to the merchant.

CREDIT CARD-BASED ELECTRONIC PAYMENT SYSTEMS

To avoid the complexity associated with digital cash and electronic cheques, consumers and vendors are looking at credit card payments on the Internet as one of the time tested alternatives.

A credit card is a small *plastic card that has* a magnetic strip on the exterior. The magnetic strip carries some form of encoded information about the card number and the card holder. The data that is encoded onto the card may be *encrypted making it difficult for potential thieves to decode or copy the information onto another card.* A card reader is required to read as well as write information to the magnetic strip.

Magnetic strip cards are vulnerable to compromise because the information is magnetically encoded and stored on the exterior of the card. *This can be copied, forged or altered.* If the data is encrypted, then the security of the information is enhanced, but the ability to exactly copy the encoded data and create a forged copy of the card is still a threat. Another drawback is that magnetically stored data is vulnerable to damage if the card is placed close to a magnet or to another magnetically encoded device. The magnetic strips are also vulnerable to scratches. However, these drawbacks have not been a deterrent to the adoption and use of magnetic strip cards. There are still widely used as credit cards, debit cards, identity cards, library cards, ATM cards etc.

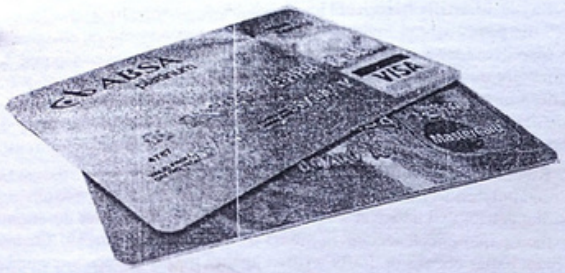


Figure 15.9 : Credit Cards

Traditionally, the credit cards were used as *off-line means* of payment. With the coming of the Internet they have been widely accepted as on-line payment mechanisms as well. Though the use of credit cards during electronic transaction added a new flavor in electronic commerce, there is nothing new in the basic process. The consumers, who want to buy a product or service, simply send their credit card details to the involving service provider and the credit card organization handles this payment like any other electronic transaction. Existing credit card-based electronic payment systems include:

(a) The use of encrypted credit cards (e.g., World Wide Web form-based encryption)

(b) Third-party authorization (e.g., First Virtual)

(a) Encryption and Credit Cards

In this scheme, in order to make a truly secure and nonrefutable transaction using an encrypted credit card, each consumer and each vendor generates a public and a secret key. The public key is sent to the credit card company and put on its public key server. The secret key is re-encrypted with a password and the unencrypted version is erased. To buy something from vendor X, the consumer sends vendor X the message, "It is now time *T*. I am paying *Y* dollars to *X* for item Z," then the consumer uses his or her password to sign the message with the public key. The vendor will then sign the message with its own secret key and send it to the credit card company, which will bill the consumer for *Y* rupees and give the same amount (less a fee) to *X*.

(b) Third-party processors and credit cards

A third party credit card processor is a company that accepts credit card orders on behalf of other online businesses. In third-party processing, consumers

register with a third party on the Internet to verify the electronic micro transactions. Here, the two key servers are merchant server and payment server. Using a client browser, a user makes a purchase from a merchant server by clicking on a payment URL (hyperlinks), which is attached to the product on a WWW page. The payment URLs send the encoded information including the details of purchase (e.g., price of item, target URL and duration) to the payment server. If the information entered by the customer is valid and funds are available, the payment server processes the payment transaction and redirects the user's browser to the purchased item with an access URL, which encodes the details of the payment transaction (the amount, what was purchased and duration). The access URL acts as a digital invoice, stamped "paid" by the payment server; which provides evidence to the merchant that the user has paid for the information and provides a receipt that grants the user access. The merchant runs an HTTP server that is modified to process access URLs. The server checks the validity of the URL and grants access if the expiration time has not passed. Once the customer is authenticated, the payment is automatically processed.

In the credit card payment system there are four players: *the customer; the vendor; the issuer and the acquire,;* The Issuer issues the customer a credit card after verifying his credentials. The issuer may or may not charge a one time or recurring processing fee from the customer. The vendor has to apply to the acquirer for permission to accept one or more *card brands.*

Pros and Cons of Credit Card Based Payments

Credit cards have advantages both for the buyer and the seller. Buyers enjoy the credit period whereas the sellers have the advantage of enhanced sales on credit cards. Also sellers are ensured that they will be paid for all their sales, they need not worry about fraud.

Drawbacks of the existing credit card-based electronic payment systems

- The credit card companies need to maintain a public server with all the public keys assuming that the credit card company will keep the vendor honest.
- The companies maintaining credit-card based payment systems have to be big enough so that the costs for management and maintenance of the system do not entail considerable profit lose. Technological and financial strength of the company need to be pretty solid.
- Requiring an on-line third-party connection for each transaction to different banks could lead to processing bottlenecks that can undermine the goal of reliable use.
- The complexity of credit card processing using an on-line third-party, takes place in the verification phase; a potential bottleneck. Verification using an OTTP is time consuming and may require many sequence-specific operations. This may lead the system at stake.

ON-LINE CARD-BASED ELECTRONIC PAYMENT SYSTEM

With a view to overcome the above stated problems associated with encrypted credit card and on-line third-party processor, in this paper, we have proposed the framework for a new electronic payment system for easy security incorporation; which does not use an on-line third party processor and which is also suitable for business implementation in the third world developing countries.

In the third world developing countries, there has been little use of e-commerce applications. Even different e-commerce applications like the electronic payment system is not that much popular in those countries. The companies and the e-commerce service providers always look for their profit. But since the cost for establishment and maintenance of the on-line third-party processor is considerably high, they are not interested to use it and as a matter of fact, the credit card-based electronic payment system using on-line third-party processor is not at all used by them.

Here is a system which explains that instead of using the on-line third-party processor how transaction can be within only two parties can be done.

In this system, there are two parties associated with a transaction. One party includes- the credit card providers (e.g., VISA, MasterCard), charge card providers (e.g., American Express), debit card providers (e.g., Bank accounts), digital card providers and private label card providers (J. C. Penny) and most importantly even the Internet Service Providers who sell prepaid cards for dialup internet access. Other party is the service provider for making on-line transactions. The consumers can get cards from the card providers who can eventually make these cards available in different stores and shops.

All the companies taking part in the card provider consortium can prepare and sell cards. But they should maintain a fixed format. Each card provider has a unique id. A card contains information about- the card provider id, secret number/ text, balance etc. Each of the companies will also maintain a database on the sold cards from where the credits will be made. Moreover, each company will maintain a server which will listen on a defined port for the 'Credit Requests'. Generally the card providers will prepare the card and will make them widely available in different shops. The cards will be ranging from very low amounts to high amounts so that users of wide verity of capability can utilize them. Each card will be bearing credit equivalent to its' cost.

The customers buy products through the web server of the service provider for making on-line transactions. The web server prompts the customers to enter their card number, password and card provider id. Ft then sends a request for crediting money to the card provider company. Where it is processed and a notification is made to the service provider about the customer balance and after getting clearance, the service provider completes the rest of the transaction, which includes keeping the record of the transaction in the form of a digital signature and requesting the deduction of credit in card sellers' database. A replica of the digital

signature is stored on the credit card provider side so that it may check this against the demand for money by the service provider at the end of the month.

A firewall will be in place between the card provider and the service provider to stand against possible threats of hacking and to prevent the intruders find also secured communication between servers are to be ensured.

Smart Cards and Electronic Payment Systems

Card technology has advanced over the years to keep ahead of the worldwide increase in card related crime. As the criminal fraternity found ways of producing sufficiently good counterfeit cards, so the card companies introduced new ways of combating the problem. A succession of anti-fraud measures have been introduced over the years such as the hologram, the Card Verification Value (C VV, a value stored on the magnetic stripe which can be used to determine if a card has been produced illicitly), and in some cases, photographs of the cardholder.

Magnetic stripe cards have now been developed to the point where there is little or no further scope for introducing more anti-crime measures. This has caused the card associations to look at new technologies to take the plastic card into the 21st century. One technology which offers many benefits is the smart card; essentially a small computer chip embedded into a plastic card with the same dimensions as the magnetic stripe card. The only difference the cardholder sees is a small metal area on the face of the card which contains a set of electrical contacts through which the chip can be accessed.

From the anti-crime perspective there are a number of benefits in adopting the smart card. The card itself (or in conjunction with the terminal) can make decisions about whether or not a transaction can take place. Secret values can be stored on the card which are not accessible to the outside world allowing for example, the card to check the cardholder's PIN without having to go online to the card issuer's host system. Also there is the possibility of modifying the way the card works while it is inserted in a point of sale terminal even to the point of blocking the card from further transactions if it has been reported lost or stolen.

As well as these anti-fraud measures, the smart card is seen as offering a number of other benefits to the card issuer and cardholder. These additional benefits are an integral part of building the business case for introducing smart card technology. Some of the other benefits of introducing smart cards are:

The ability to have more than one payment application resident on the card. For example a card could contain an "electronic purse" to provide the equivalent of cash, usually for lower value transactions such as parking, tickets, newspapers etc.

The ability to have other applications such as loyalty schemes and access to information facilities (e.g. libraries) co-resident on the card.

The possibility of reducing on-line validation costs by allowing the card to operate off-line more of the time.

In the future there may be the possibility of storing personal details such as driving license and medical records on the card.

There are many issues to be resolved before such all-embracing cards become common place, the most obvious ones being who owns the card and who controls which applications can be loaded or deleted.

Today, the banks are interested mainly in providing payment related services to their customers and most of the current activity surrounds the provision of smart card based credit/debit services sometimes with an additional electronic purse facility.

Smart cards have been in existence since the early 1980s and have become a widely accepted and secure means of handling off-line as well as on-line transactions.

A smart card is a small plastic card that looks similar to a credit card, but it contains a microprocessor and a storage unit.

Or

A smart card, chip card, or **integrated circuit card** (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information. This implies that it can receive input which is processed - by way of the ICC applications - and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally PVC, but sometimes ABS. The card may embed a hologram to avoid counterfeiting.

Figure 15.10 : Smart Card

Smart card technology has been able to overcome most of the limitations of the magnetic strip cards, however they are more expensive to issue. The stored data is not externally exposed to physical damage, such as scratches, and it is not vulnerable to damage from magnetic fields. Further smart cards can store significantly *greater amounts of data,* estimated to be almost 100 times, than the magnetic strip cards.

Smart cards are basically of two types :

1. Memory smart cards or electronic purses or Debit cards.
2. Intelligent or Relationship-based smart cards.

Electronic Purses

Electronic purses are smart cards that are capable of storing monetary value onto their microprocessor chip. The consumers for purchase can use this money. These are used as debit cards for the payment against purchase of goods/ services or as pre- paid telephone cards.

The memory smart cards or electronic purses contain less information and processing capabilities than the intelligent smart cards.

Smart cards can be loaded with money at an ATM equipped with a smart card reader or a special machine by either putting in cash or credit card. Vendors accepting smart cards as a form of payment must be equipped with a smart card reader. Many smart card readers are compatible with magnetic strip card readers.

Smart card technology can be used in either on-line or off-line mode. An off-line smart card operates in the following manner:

1. The consumer pays for the goods/services purchased by inserting the smart carq into the vendor's smart card reader.
2. If there is enough money available for the purchase made, the value of the purchase is deducted from the balance on the card and added to an e-cash box on the vend- ing machine. The remaining balance on the card is displayed on the vending ma- chine or can be checked at an A TM or a balance reading device.

And when the balance on an electronic purse is depleted, the purse can be recharged with more money. As for the vendor, at the end of the day or periodically he inserts smart card into the vending machine or card reader to download the sales. He can take the smart card to his bank and by inserting it into an ATM or smart card reader he can redeem his cash or get the money transferred into his bank account.

The smart card technology may also be used *on-line from the customers personal* computer if a smart card slot and the relevant software are available. The user can then use the smart card for purchase with any vendor who accepts the smart card payment on-line using some relevant software. The vendor's PC must also be equipped with a card reader to enable him to load the payments in his smart card for credit or the vendor may have an on-line connection with the bank for credit of the payments.

Protection of Smart cards may done from theft and misuse by having identification pictures on them or through password protection.

Such pre-paid systems are preferred by the vendors as there are less chances of fraud. Also they are good for the banks or financial institutions in comparison to credit cards as the bank does not have to pay interest on the money any more.

Relationship-Based Smart Cards

Relationship based smart cards are enhanced smart cards that store cardholder information including *name, birth date, personal shopping preferences and actual purchase records*. Such information would enable merchants to accurately track consumer behavior and develop promotional programs designed to increase the shopper loyalty. Relationship-based smart cards are expected to offer consumers far greater options, including the following:

Access to multiple services such as debit, credit, investments or stored value for e-cash on a single card.

- A variety of functions, such as cash access, bill payment, balance inquiry or funds transfer for selected accounts.
- Multiple services at multiple locations using multiple device types, such as an auto- mated teller machine, a screen phone, a personal computer, a personal digital assistant (PDA) etc.
- Online payments of Reservations of railways; airways, shopping etc.

Companies are trying to incorporate these services into a personalized banking relationship for each customer to enhance convenience, building loyalty and retention and attract new customers. Bank are also attempting to customize services on smart cards, offering a menu of services similar to those that come up on ATM screens. As with credit cards, banks may also link up with health care providers, telephone companies, online shops, web merchants, travel agencies, hotels, retailers and airlines to offer frequent shopping and other related services.

Place	Card	Provider	Introduction Year
Delhi	Delhi Metro Smart Card	Delhi Metro Rail Corp	2005
Delhi	Driving License Smart Card (ongoing tender)	Government of India	2007
Delhi	Vehicle Registration Certificate Smart Card	Government of India	2005
Jamshedpur	Xavier Labor Relations Institute smart card	XLRI Card	2006
Kolkata	Kolkata Metro Smart Card	Kolkata Metro Rail Corp.	
Mumbai	Bus Pass Smart Card	BEST (Brihan Mumbai Electric Supply & Transport Undertaking)	2007

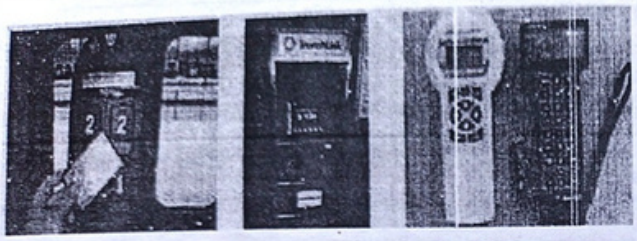
Table 1 : Use of Smart Cards in India .

Smart Card Readers and Smart Phones

The benefits of smart cards will rely greatly on the omni-presence of devices called the smart card readers that can communicate with the chip on the smart card. In addition to reading from and writing to the smart cards, these devices can also combine the elements of a personal computer, a point-of-sale terminal and a phone to allow consumer to quickly conduct financial transaction without leaving their homes.

In the simplest form, a card reader features a two-line by 16 character display that can show both a prompt and the response entered by the user. Efficiency is further enhanced by color-coded function keys, which can be programmed to perform the frequently used operations in a single keystroke. The card reader can communicate via RS-232 serial interface with any transaction automation system, including PCs and electronic cash registers.

Recently card readers in the form of screen phones are becoming very popular. The screen-based phones feature a four-line screen, a magnetic strip card reader, a phone keypad and a keyboard. The *screen* phones offer user interface through menus similar to those found on ATMs. Other features of screen phones include advanced telephonic functions such as atwo-way speaker phone capability, a dialling directory at a phone log for tracking calls.



Figures 15.11 : Smart Card Readers 1, 2, 3

To promote smart card usage the smart card forum group of about 130 businesses and government agencies is drawing up common specifications to promote the use of multiple application smart cards useable almost everywhere, from micro payments to large business payments.

Business Issues and Smart Cards

Cash is expensive to handle, count, and deposit and many involve theft, fraud or misplacement. As an alternative, smart cards are very convenient alternative to handling cash.

Also in banking systems it has been estimated that about 4 percent of the value of cash that is deposited gets used up in handling costs. As a long-term planning the bank industry forecasts the closing of the many expensive branches and conducting virtually all business by telephone, using cash machines and home computers, thus weaning away of even the small businesses and consumers of cash.

Electronic purses are already very popular in the advanced countries to pay for small as well as big items/services. Mondex, a more advanced usage of smart cards, are electronic purses that can be loaded with five currencies at one time. Like cash and unlike most other electronic purse systems, Mondex is anonymous. The banks that issue Mondex cards will not be able to keep track of who makes or receives payments.

QUESTIONS

Very Short Questions :

1. What is payment Gask way ?
2. What is SET ?
3. What is blinding factor ?
4. What is Diversibility ?
5. What is Interoperability ?
6. What is Non-refutability ?
7. What is Anonymity ?

Short Questions :

1. What do you mean by EFT ?
2. What do you mean by E-Cagn ?
3. Explain the Pros and Cons of Credit Card Based Payment ?
4. What do you mean by Electronic Purse ?
5. What is relationship based Emart cards ?
6. Write a process to purchase e-cash ?

Long Question :

1. What do you mean by Third Party Authentication, Discuss in detail.
2. What do you mean by EFT ? Discuss in detail.
3. How you purchase e-cash and how it will work ?
4. Explain all properties and Specification of Digital Currencies.
5. What is the difference between Debit Card, Credit Card & Smart Card.

❑❑❑

16

Security Issues In Ecommerce

Introduction

E-commerce is defined as the buying and selling of products or services over electronic systems such as the Internet and to a lesser extent, other computer networks. It is generally regarded as the sales and commercial function of eBusiness. There has been a massive increase in the level of trade conducted electronically since the widespread penetration of the Internet. A wide variety of commerce is conducted via eCommerce, including electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

E-commerce tends to be at a higher echelon for risk and attacks. This is so because according to our definition, E-Commerce is the transaction of goods and services; and the payment for those goods and services over the Internet. Therefore, the physical place where all of these transactions occur is at the Server level. The server can be viewed as the central repository for your "E-Commerce Place of Business"[which consists of the actual website which displays your products and services, the customer database, and the payment mechanism]. If there are any attacks to this server, in one blow, there is the potential you could lose everything. Thus, being proactive about security takes on a much greater magnitude now.

Threats to E-Commerce servers fall into two general categories:

(1) Threats from an actual attacker(s); and

(2) Technological failure.

In terms of the former, the motivation is primarily psychological. The intent is to garner personal information from people for the sheer purposes of exploitation (such obtaining Credit Card and Bank Account information, Phishing schemes, obtaining usernames and passwords, etc.). With the latter, anything related to the Internet can cause problems. This can be anything from a network not configured

properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your E-Commerce site was developed can be very susceptible to threats. Most E-Commerce Servers utilize a Windows Operating System (such as Windows 2000 and 2003 Server), a Web Server Software to host the E-Commerce Site (such as Internet Information Services, or IIS), and a database (such as Access 2000 or SQL Server 2000) which contains your customer information and transaction history. These platforms have had various security flaws associated with them, which has made them wide open to threats and attacks. As a result, there has been a move in the business community to adopt more robust and secure platforms. A prime example of this is the use of Linux as the operating system, Apache as the Web Server Software, and either PostGRESql or My SQL as the database (these are database languages created from the Structured Query Language, or SQL).

Threats to Ecommerce

The direct threats to E-Commerce servers can be classified as either

(1) Malicious Code Threats; and

(2) Transmission Threats.

With the former, malicious, or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server. With the latter, the threats and risks can be classified as either as active or passive. With passive threats, the main goal is to listen (or eavesdrop) to transmissions to the server. With active threats, the intent is to alter the flow of data transmission or to create a rogue transmission aimed directly at the E-Commerce server.

There are several types of attacks that a hacker can choose to deploy. Some attacks aim at gaining specific information on individuals or companies to do harm to. Other types can just shut down the network so it is in operable which could cause a business to lose on revenues. Some of these attacks are easily repairable and others can cause a significant amount of damage to individuals and to companies.

(1) Malicious Code Attacks

Malicious or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server. Malware is very much a part of the digital online landscape no matter it is welcome or not.

Malicious Software

Malware

Malware is malicious software. This software include the program that exploit the vulnerabilities in computing system. The purpose of malicious software is harm you or steal the information from you.

Malicious Software is also commonly referred to as Malware. According to Bruce Schneier, "Malicious Software includes computer viruses, worms, and trojan horses". Other experts include spyware, dishonest adware, crimeware, rootkits, and other unwanted software. Bots and botnets will also be presented as they have also become a more common threat to computer security.

What is it? Malicious Software or malware is software designed to infiltrate a computer system without the owner's informed consent.

What does it do? Depending on the variety of malware, "it can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up". The bottom line is malware can cost you or your organization time, money, resources, privacy, and security.

There are three characteristics of malwares:

1 Self-replicating malware actively attempts to propagate by creating new copies, or instances, of itself. Malware may also be propagated passively, by a user copying it accidentally, for example, but this isn't self-replication.

2 The population growth of malware describes the overall change in the number of malware instances due to self-replication. Malware that doesn't self replicate will always have a zero population growth, but malware with a zero population growth may self-replicate.

3 Parasitic malware requires some other executable code in order to exist. "Executable" in this context should be taken very broadly to include anything that can be executed, such as boot block code on a disk, binary code

Virus:

Self-replicating: yes

Population growth: positive

Parasitic: yes

A virus is malware that, when executed, tries to replicate itself into other executable code; when it succeeds, the code is said to be infected. The infected code, when run, can infect new code in turn. This self-replication into existing executable code is the key defining characteristic of a virus.

Types of Viruses

Viruses have been categorised into several different types according to the ways in which they infect a system, the part of the system they affect or their behaviours.

Parasitic virus:

Traditional and common virus. This will be attached with EXE files and search for other EXE file to infect them.

Memory Resident Virus:

Present in your system memory as a system program. From here onwards it will infects all program that executes.

Boot Sector Virus:

Infects the boot record and spread when the system is booted from the disk containing the virus.

Stealth Virus:

This virus hides itself from detection of antivirus scanning.

File Infector Viruses

File infector viruses are those that infect other files or programs on your system. They operate in a number of ways. Once the original 'host' program is run, the virus can stay resident or 'live' inside your systems memory (RAM) and infect programs as they are opened, or they can lay dormant inside another program. Each time that program is run, the virus will infect another program or file.

A second, more complex file infector is one that doesn't alter the program itself, but alters the route a computer takes to open a file. In this way, the virus is executed first, and then the original program is opened. If a program or file that is infected with a file infector virus is passed from one computer to another, over a network or via floppy disk for example, the virus will begin infecting the 'clean' computer as soon as the file or program is opened.

Boot Sector Viruses

Whereas file infector viruses infect programs on a computer's hard drive, boot sector viruses can infect hard drives and removable disks, such as floppy disks. The boot sector is an area at the beginning of a hard drive or other disk where information about the drive or disk structure is stored. Symptoms of a boot sector virus may be a computer that is unbootable or gives error messages upon booting. Frustratingly, boot sector viruses may be present with no noticeable problems.

One thing should be noted about floppy disks. It does not matter whether the floppy disk is a 'bootable' disk or not, if the disk is infected with a boot sector virus and you inadvertently leave the disk in the drive when you reboot the computer, the virus can still be executed. Ways of preventing this will be discussed in part two of this series.

Macro Viruses

Macro viruses are by far the most common type of malicious code found today. This is due to the popularity of software such as Microsoft Office and others such as Corel Draw, which use the macro programming languages extensively in the products.

Macro viruses use an application's own macro programming language to distribute themselves. Macro viruses do not infect programs; they infect documents. Macro viruses typically arrive in an infected document, a price list written with MS Word for example. When the file is opened, the virus infects the base template on the victim computer, in this case Normal.dot. Normal.dot is the 'framework' that Word documents are created on. Once this template is infected, every document that is opened from then on will be infected as well, making all documents created or opened in Word a carrier of the macro virus. Macro viruses have been written for most Microsoft Office applications, including Excel, Access, PowerPoint and Word. They can also be found in Lotus AmiPro and Corel products to name a few.

One more warning about macro viruses is that they are not platform specific. They can be found and spread through Macintosh, DEC Alpha, Microsoft NT and Microsoft Windows. In other words, just because you received a Microsoft Word file from a colleague using a Macintosh, doesn't mean you will not be infected by a macro virus embedded in that document.

Worms

Self-replicating: yes

Population growth: positive

Parasitic: no

A worm shares several characteristics with a virus. The most important characteristic is that worms are self-replicating too, but self-replication of a worm is distinct in two ways. First, worms are standalone, and do not rely on other executable code. Second, worms spread from machine to machine across networks.

A worm is a piece of code that can make fully functional copies of itself and travel through a computer network and/or across the Internet through a number of means. A worm does not attach themselves to other programs like traditional viruses, but creates copies of itself, which in turn create even more copies. The computer 'worm' is so-called because of the way in which 'rogue' computer code was originally detected. Printouts of computer memory locations would show random 'wormhole' patterns, much like that of the patterns on worm-eaten wood. The term eventually became shortened and used to describe viruses that could 'worm' or propagate across networks and the Internet, leaving copies of themselves as they travelled.

Worms are prolific due to the fact that most are created using simple scripting languages that can be created with a text editor and become fully functional 'programs' under the right conditions. For example, if you were to obtain a copy of the 'I Love You' worm and changed the files extension from vbs to txt, you could safely open the file in Notepad and view the structure of the worm. This makes the vbs script worm extremely popular among the 'script kiddy' fraternity, as it takes no (or very little) programming knowledge to modify an existing worm and release it

into the wild (when a virus is circulating in the computing community or throughout the Internet, it is said to be 'in the wild'.)

Trojan Horses

Self-replicating: no

Population growth: zero

Parasitic: yes

Trojan horses are named after the wooden horse from Greek mythology in which Greek soldiers snuck into the city of Troy. Accordingly Trojans are malicious programs that sneak into a victim computer disguised as harmless software. Trojans may also be 'wrapped' inside another program so that when the original innocent program is installed, the Trojan program is installed as well.

The most commonly described Trojan has a payload that will allow a user on another computer somewhere else in the world to gain full control and access to the files on your computer. In this way, they can be used to launch denial of service attacks such as those that brought down Yahoo! and E-bay early in 2000.

Trojan horses typically consist of two parts, the server and the client. The server is the part that is installed on the victim computer. When the server is installed, it allows the remote client to send commands to the computer as if the other person were sitting at the keyboard. The remote attacker can upload and download files, delete and create files on your system, play with the CD drive and generally control most aspects of the victim machine. Most of the approximately 550 known Trojans will send some sort of message to the attacker to let them know the server is running on the computer. Therefore, every time you connect to the Internet the person who sent the Trojan will know that the system is online and open for abuse.

Legal Risks Associated with Trojan Infections

In addition to the effects previously mentioned, a Trojan infection may affect you legally. If your network has been used surreptitiously by an attacker as a launching pad for a denial of service or other attack, you may be held responsible for any legal damages. Further, a Trojan on your system could be used to gain access to another network to steal sensitive information. If the intrusion is traced back to your computer, it may be difficult and expensive to defend yourself against prosecution.

There is also the risk of losing your sensitive business information; contacts, blueprints, liabilities, etc to a competitor eager to gain an advantage over you. Imagine how easy it would be for a competitor to undercut you if they had access to all your customer accounts and contact details.

Hoax Viruses

There are hundreds of hoax viruses that spread like chain letters through e-mail. Although they cause little or no long-term damage, these hoaxes can be as

disruptive as real malicious code. The standard response of most people when receiving a virus warning is to pass it on to all people in their organisation and most likely everyone else in their contacts lists. This sets up a chain reaction that not only wastes Internet bandwidth, but also wastes the valuable time of recipients.

Further, a hoax can be damaging to a company's reputation. For example, NVision Design Inc produced three small games prior to Christmas of 1999. A virus hoax was spread worldwide that these games (Frog-a-pult, Elf-Bowl and Y2K game) contained a delayed action virus that would wipe out the users hard-drive. Not only did this cause damage to the reputation of the games' developer Vectrix, it also caused a deluge of e-mails in peoples' mail servers and inboxes.

Logic Bomb:

Self-replicating: no

Population growth: zero

Parasitic: possibly

The oldest type of malicious software. This program is embedded with some other program. When certain condition meets, the logic bomb will destroy your pc. It also crash at particular date which is fixed by attacer. Eg: if some antivirus trying to delete or clean the logic bomb. The logic bomb will destroy the pc.

Back Door or Trap Door:

Self-replicating: no

Population growth: zero

Parasitic: possibly

A back door is any mechanism which bypasses a normal security check. Programmers sometimes create back doors for legitimate reasons, such as skipping a time-consuming authentication process when debugging a network server.

One special kind of back door is a RAT, which stands for Remote Administration Tool or Remote Access Trojan, depending on who's asked. These programs allow a computer to be monitored and controlled remotely;

Rabbit:

Self-replicating: yes

Population growth: zero

Parasitic: no

Rabbit is the term used to describe malware that multiplies rapidly. Rabbits may also be called bacteria, for largely the same reason.

There are actually two kinds of rabbit.The first is a program which tries to consume all of some system resource, like disk space. A "fork bomb," a program which creates new processes in an infinite loop, is a classic example of this kind of

rabbit. These tend to leave painfully obvious trails pointing tothe perpetrator, and are not of particular interest.

The second kind of rabbit, which the characteristics above describe, is a special case of a worm. This kind of rabbit is a standalone program which replicates itself across a network from machine to machine, but deletes the original copy of itself after replication. In other words, there is only one copy of a given rabbit on a network; it just hops from one computer to another. Rabbits are rarely seen in practice.

Spyware:

Spyware is software which collects information from a computer and transmits it to someone else.

The exact information spyware gathers may vary, but can include anything which potentially has value:

1. Usernames and passwords. These might be harvested from files on the machine, or by recording what the user types using a key logger. A keylogger differs from a Trojan horse in that a keylogger passively captures keystrokes only; no active deception is involved.
2. Email addresses, which would have value to a spammer.
3. Bank account and credit card numbers.
4. Software license keys, to facilitate software pirating.

Adware:

Self-replicating: no

Population growth: zero

Parasitic: no

Adware has similarities to spyware in that both are gathering information about the user and their habits. Adware is more marketing-focused, and may pop up advertisements or redirect a user's web browser to certain web sites in the hopes of making a sale. Some adware will attempt to target the advertisement to fit the context of what the user is doing. For example, a search for "Calgary" may result in an unsolicited pop-up advertisement for "books about Calgary." Adware may also gather and transmit information about users which can be used for marketing purposes. As with spyware, adware does not self-replicate.

Zombies:

Computers that have been compromised can be used by an attacker for a variety of tasks, unbeknownst to the legitimate owner; computers used in this way are called zombies. The most common tasks for zombies are sending spam and participating in coordinated, large-scale denial-of-service attacks.

Macro viruses use an application's own macro programming language to distribute themselves. Macro viruses do not infect programs; they infect documents. Macro viruses typically arrive in an infected document, a price list written with MS Word for example. When the file is opened, the virus infects the base template on the victim computer, in this case Normal.dot. Normal.dot is the 'framework' that Word documents are created on. Once this template is infected, every document that is opened from then on will be infected as well, making all documents created or opened in Word a carrier of the macro virus. Macro viruses have been written for most Microsoft Office applications, including Excel, Access, PowerPoint and Word. They can also be found in Lotus AmiPro and Corel products to name a few.

One more warning about macro viruses is that they are not platform specific. They can be found and spread through Macintosh, DEC Alpha, Microsoft NT and Microsoft Windows. In other words, just because you received a Microsoft Word file from a colleague using a Macintosh, doesn't mean you will not be infected by a macro virus embedded in that document.

Worms

Self-replicating: yes

Population growth: positive

Parasitic: no

A worm shares several characteristics with a virus. The most important characteristic is that worms are self-replicating too, but self-replication of a worm is distinct in two ways. First, worms are standalone, and do not rely on other executable code. Second, worms spread from machine to machine across networks.

A worm is a piece of code that can make fully functional copies of itself and travel through a computer network and/or across the Internet through a number of means. A worm does not attach themselves to other programs like traditional viruses, but creates copies of itself, which in turn create even more copies. The computer 'worm' is so-called because of the way in which 'rogue' computer code was originally detected. Printouts of computer memory locations would show random 'wormhole' patterns, much like that of the patterns on worm-eaten wood. The term eventually became shortened and used to describe viruses that could 'worm' or propagate across networks and the Internet, leaving copies of themselves as they travelled.

Worms are prolific due to the fact that most are created using simple scripting languages that can be created with a text editor and become fully functional 'programs' under the right conditions. For example, if you were to obtain a copy of the 'I Love You' worm and changed the files extension from vbs to txt, you could safely open the file in Notepad and view the structure of the worm. This makes the vbs script worm extremely popular among the 'script kiddy' fraternity, as it takes no (or very little) programming knowledge to modify an existing worm and release it

into the wild (when a virus is circulating in the computing community or throughout the Internet, it is said to be 'in the wild'.)

Trojan Horses

Self-replicating: no

Population growth: zero

Parasitic: yes

Trojan horses are named after the wooden horse from Greek mythology in which Greek soldiers snuck into the city of Troy. Accordingly Trojans are malicious programs that sneak into a victim computer disguised as harmless software. Trojans may also be 'wrapped' inside another program so that when the original innocent program is installed, the Trojan program is installed as well.

The most commonly described Trojan has a payload that will allow a user on another computer somewhere else in the world to gain full control and access to the files on your computer. In this way, they can be used to launch denial of service attacks such as those that brought down Yahoo! and E-bay early in 2000.

Trojan horses typically consist of two parts, the server and the client. The server is the part that is installed on the victim computer. When the server is installed, it allows the remote client to send commands to the computer as if the other person were sitting at the keyboard. The remote attacker can upload and download files, delete and create files on your system, play with the CD drive and generally control most aspects of the victim machine. Most of the approximately 550 known Trojans will send some sort of message to the attacker to let them know the server is running on the computer. Therefore, every time you connect to the Internet the person who sent the Trojan will know that the system is online and open for abuse.

Legal Risks Associated with Trojan Infections

In addition to the effects previously mentioned, a Trojan infection may affect you legally. If your network has been used surreptitiously by an attacker as a launching pad for a denial of service or other attack, you may be held responsible for any legal damages. Further, a Trojan on your system could be used to gain access to another network to steal sensitive information. If the intrusion is traced back to your computer, it may be difficult and expensive to defend yourself against prosecution.

There is also the risk of losing your sensitive business information; contacts, blueprints, liabilities, etc to a competitor eager to gain an advantage over you. Imagine how easy it would be for a competitor to undercut you if they had access to all your customer accounts and contact details.

Hoax Viruses

There are hundreds of hoax viruses that spread like chain letters through e-mail. Although they cause little or no long-term damage, these hoaxes can be as

disruptive as real malicious code. The standard response of most people when receiving a virus warning is to pass it on to all people in their organisation and most likely everyone else in their contacts lists. This sets up a chain reaction that not only wastes Internet bandwidth, but also wastes the valuable time of recipients.

Further, a hoax can be damaging to a company's reputation. For example, NVision Design Inc produced three small games prior to Christmas of 1999. A virus hoax was spread worldwide that these games (Frog-a-pult, Elf-Bowl and Y2K game) contained a delayed action virus that would wipe out the users hard-drive. Not only did this cause damage to the reputation of the games' developer Vectrix, it also caused a deluge of e-mails in peoples' mail servers and inboxes.

Logic Bomb:

Self-replicating: no

Population growth: zero

Parasitic: possibly

The oldest type of malicious software. This program is embedded with some other program. When certain condition meets, the logic bomb will destroy your pc. It also crash at particular date which is fixed by attacer. Eg: if some antivirus trying to delete or clean the logic bomb. The logic bomb will destroy the pc.

Back Door or Trap Door:

Self-replicating: no

Population growth: zero

Parasitic: possibly

A back door is any mechanism which bypasses a normal security check. Programmers sometimes create back doors for legitimate reasons, such as skipping a time-consuming authentication process when debugging a network server.

One special kind of back door is a RAT, which stands for Remote Administration Tool or Remote Access Trojan, depending on who's asked. These programs allow a computer to be monitored and controlled remotely.

Rabbit:

Self-replicating: yes

Population growth: zero

Parasitic: no

Rabbit is the term used to describe malware that multiplies rapidly. Rabbits may also be called bacteria, for largely the same reason.

There are actually two kinds of rabbit.The first is a program which tries to consume all of some system resource, like disk space. A "fork bomb," a program which creates new processes in an infinite loop, is a classic example of this kind of

rabbit. These tend to leave painfully obvious trails pointing tothe perpetrator, and are not of particular interest.

The second kind of rabbit, which the characteristics above describe, is a special case of a worm. This kind of rabbit is a standalone program which replicates itself across a network from machine to machine, but deletes the original copy of itself after replication. In other words, there is only one copy of a given rabbit on a network; it just hops from one computer to another. Rabbits are rarely seen in practice.

Spyware:

Spyware is software which collects information from a computer and transmits it to someone else.

The exact information spyware gathers may vary, but can include anything which potentially has value:

1. Usernames and passwords. These might be harvested from files on the machine, or by recording what the user types using a key logger. A keylogger differs from a Trojan horse in that a keylogger passively captures keystrokes only; no active deception is involved.
2. Email addresses, which would have value to a spammer.
3. Bank account and credit card numbers.
4. Software license keys, to facilitate software pirating.

Adware:

Self-replicating: no

Population growth: zero

Parasitic: no

Adware has similarities to spyware in that both are gathering information about the user and their habits. Adware is more marketing-focused, and may pop up advertisements or redirect a user's web browser to certain web sites in the hopes of making a sale. Some adware will attempt to target the advertisement to fit the context of what the user is doing. For example, a search for "Calgary" may result in an unsolicited pop-up advertisement for "books about Calgary." Adware may also gather and transmit information about users which can be used for marketing purposes. As with spyware, adware does not self-replicate.

Zombies:

Computers that have been compromised can be used by an attacker for a variety of tasks, unbeknownst to the legitimate owner; computers used in this way are called zombies. The most common tasks for zombies are sending spam and participating in coordinated, large-scale denial-of-service attacks.

(2)Transmission Threats

Denial of Service Attacks

With a Denial of Service Attack, the main intention is to deny your customers the services provided on your E-Commerce server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a massive amount of invalid data is sent to the server. Because the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes "confused", and subsequently shuts down. Another type of Denial of Service Attack is called the Distributed Denial of Service Attack. In this scenario, many computers are used to launch an attack on a particular E-Commerce server. The computers that are used to launch the attack are called "zombies." These "zombies" are controlled by a master host computer. It is the master host computer which instructs the "zombie" computers to launch the attack on the E-Commerce Server. As a result, the server shuts down because of the massive bombardment of bad information and data being sent from the "zombie" computers. A Distributed Denial of Service Attack is diagrammed as follows:

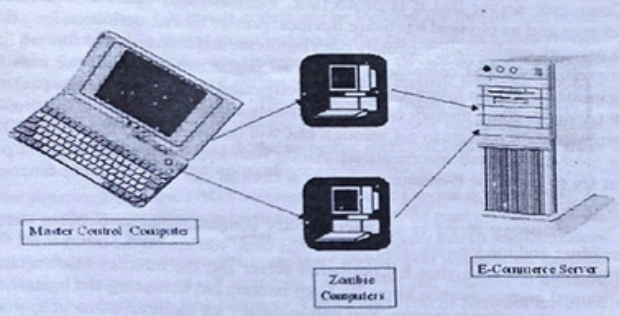


Fig. : 16.1 Diagram of A Distributed Denial of Service Attack

Ping of Death

When we surf the Web, or send E-Mail, the communications between our computer and the server takes place via the data packet. It is the data packet that contains the information and the request for information that is sent from our computer to other computers over the Internet. The communication protocol which is used to govern the flow of data packets is called Transmission Control Protocol/Internet Protocol, or TCP/IP for short. The TCP/IP protocol allows for data packets to be as large as 65,535 bytes. However, the data packet size that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a massive data packet is sent-65,536 bytes. As a result, the memory buffers of the E-Commerce Server are totally overloaded, thus causing it to crash.

SYN Flooding

When we open up a Web Browser and type in a Web address, or click "Send" to transmit that E-Mail from our own computer (referred to as in this section as the "client computer"), a set of messages is exchanged between the server and the client computer. These set of exchanges is what establishes the Internet connection from the client computer to the server, and vice versa. This is also known as a "handshake." To initiate this Internet connection, a SYN (or synchronization) message is sent from the client computer to the server, and the server replies back to the client computer with a SYN ACK (orsynchronization acknowledgement) message. To complete the Internet connection, the client computer sends back an ACK (or acknowledgement) message to the server. At this point, since the E-Commerce server is awaiting to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point in which the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server, thus overloading its memory and processing power, and causing it to crash.

Threats to Your E-Commerce Customers

Phishing Attacks

One of the biggest threats to your E-Commerce customers is that of Phishing. pecifically, Phishing can be defined as the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. So, for example, fraudulent e-mail could be sent to your customers claiming that their online account is about to expire, or their username and password has been compromised in some fashion, or that there is a security upgrade that will take place affecting their online account. After they are tricked into believing the content of the Phishinig e-mail, the customer then clicks on the link, and submits all of their confidential information. All Phishing e-mail contains a link, or a web address, in which the customer clicks on thinking that they are going to secure and legitimate site (people who launch Phishing schemes [also known as "Phishers"] can copy the HTML code from your E-Commerce site, making it look authentic in the eyes of the customer). The truth is, all of the confidential information submitted is collected by the "Phisher", who is bent upon creating havoc and damage to your E-Commerce business.

Other Threats to E-Commerce Servers

There are other threats posed to E-Commerce servers, a few are listed here. These threats will be further discussed in subsequent articles.

Data Packet Sniffing

This refers to the use of Data Packet Sniffers, also known simply as "sniffers." While it is an invaluable tool to the Network Administrator for troubleshooting and diagnosis, an attacker can also use a sniffer to intercept the data packet flow and analyze the individual data packets. Usernames, passwords, and other confidential customer data can then be hijacked from the E-Commerce server. This is a very serious problem, especially in wireless networks, as the data packets literally leave the confines of the network cabling and travel in the air. Ultimately, Data Packet Sniffing can lead to hijacking sessions. This is when the attacker eventually takes control over the network connection, kicks off legitimate users (such as your customers) from the E-Commerce server, and ultimately gains control of it.

IP Spoofing

The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With IP Spoofing, it is difficult to identify the real attacker, since all E-Commerce server logs will show connections from a legitimate source. IP Spoofing is typically used to start the launch of a Denial of Service Attack.

Port Scanning

This is listening to the network ports of the E-Commerce server. When conducting such a scan, an attacker can figure out what kind of services are running on the E-Commerce server, and from that point figure out the vulnerabilities of the system in order to cause the greatest damage possible.

Trapdoors/Backdoors

In developing the code for an E-Commerce site, developers often leave "trapdoors" or "backdoors" to monitor the code as it is developed. Instead of a implementing a secure protocol in which to access the code, backdoors provide a quick way into the code. While it is convenient, trapdoors can lead to major security threats if they are not completely removed prior to the launch of the E-Commerce site. Remember, an attacker is always looking first for vulnerabilities in the E-Commerce server. Trapdoors provide a very easy vulnerability for the attacker to get into, and cause system wide damage to the E-Commerce server.

Security Tools

Preventative Strategies

When it comes to protecting company's stored data on the computer, protective strategies takes place. It is a sad but true statement when I say that the

"good guys" of IT security are constantly playing catch up with the hackers and attackers. The hackers and attackers are constantly coming up with new techniques to try and gain illegal access to information, and as a result IT security professionals need to be on their toes looking for new attacks and ways to prevent them. IT security professionals cannot guess what type of attack will be discovered next, they have to wait for these attacks to surface so they can attempt to deploy new tactics of fighting off the attacks. This next section is going to discuss the commonly used preventative strategies that are being deployed by IT security officials today to thwart against hackers attempts at causing mayhem and destruction on the e-Commerce servers. These are tools that are designed to protect valuable information that is traveling across servers and networks.

(I) Firewalls

A firewall is a very important tool to use to protect personal information and company data as well. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The firewall acts as security checkpoint that all communication with your server has to cross through. It is a very effective spot to impose security rules. A firewall is like a bodyguard that information and data from outside the network needs to pass through and get inspected by before the data and information can be passed onto the ECommerce server that it is protecting. Firewalls can come both as software packages and as physical hardware devices. A more formal definition for a firewall is a network configuration, usually both hardware and software that forms a fortress between networked computers within an organization and those outside the organization. So the firewall acts like a bodyguard, by examining data packets that are trying to come through onto the E-commerce server. It will allow proper and legitimate data packets to get through but will deny access to data packets that do not meet the firewall specifications. Along with inspecting all of the data packets that try to enter the E-commerce server a firewall can also serve the function of a proxy server.

A proxy server is an intermediary computer that is between the user's computer and the Internet. This means that when you are on the internet the firewall is standing between your E-Commerce server and the internet blocking bad and unwanted communication attempts from hackers but accepting the legitimate ones that you are trying to initiate. You can manually set the level of security you want the firewall to use. Maximum security will block all access to the server from the outside. Minimal security will allow too much access. You need to determine how much security you will need when you set up your firewall and you can add or remove certain security features overtime as you realize that you may or may not need them. The Firewall can also provide valuable information to the Systems Administrator, such as the types and amount of data packet traffic, number of attempted network break ins, etc. It is important to know that firewalls are very

good at protecting your server from outside attacks, it does not protect against an internal threat, such as a disgruntled employee. Frequently monitoring the firewall is probably a good idea to make sure there are no internal attacks on the network.

(II) Routers

Earlier in the last section it was mentioned that a firewall can come in software packages or as a physical hardware device. A router is an example of a firewall in hardware form. Routers are devices that computers and servers on the network can connect to, to have access to the network. Routers are used to accomplish two main goals: (1)It is a Firewall, so it protects the network and the ECommerce Servers, and (2)Routers insure that data packets do not go where there are not intended to, and make sure that they arrive where there are intended to. The Router will decide which path in the network to send the data packets so they end up at the desired location in the fastest time. Routers also have an additional level of security over software firewalls because they have a Network Address Translation (NAT) feature in which it will disguise your servers IP address to the outside world and show the routers IP address instead.

(III) Network Intrusion Devices

A Network Intrusion Device (IDS) is a device that takes the role in not only defending your network but it will constantly be looking for threats both inside and outside the network. If a threat is picked up by the Network Intrusion Device then it will alert the security professionals monitoring the device so they can decide what security measures to implement on the intrusion. Network Intrusion Devices can come in two different ways with different security features being unique to each one. The first one, called "NIDS" for Network Based Intrusion Detection Device, is usually used to look through the incoming data packets to inspect them before they make contact with the network.

One drawback with the NIDS Network Intrusion Device is that as your E-commerce networks are gaining in growth and the number of packets increases the NIDS must have enough room to support the growth. So if you start a small business that does not get a lot of communication on your server, you might want to make sure that if your business takes off that you can handle the changes in network traffic that will be coming with new business. The second type of Network Intrusion Device is called "HIDS" for Host Based Intrusion Detection Device. This HIDS is connected to only a single server or computer, as compared to a NIDS which is connected to a network of computers and servers. HIDS will more than likely be used for smaller personal protection while NIDS should be used for more organized E-commerce transactions.

(IV) Authentication

When your customer logs onto your E-commerce server, they are logging on assuming that they are going to a secure valid site. From the owner's point of

view, they will want to ensure that the right authorized user is logging on and not some hacker trying to gain access through the user. Authentication is what we use to describe this. Authentication is verification who the user is and whether the user is allowed access to the network.

To process through Authentication we use something called Secure Sockets Layer, "SSL". Secure Socket Layer uses digital certificates that are sent between the two servers, or the computer and server that are trying to make contact with each other. The Secure Sockets Layer is frequently used to control the security of messages being sent over the internet. SSL has been improved to something called Transport Layer Security which was founded on the same principles of SSL. "TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS. SSL and TLS should be used on an E-Commerce website when a customer must input a username and password, and also if they have to give credit card information. Even though today obtaining a SSL, secure socket layer, certificate is very easy and costless some online shopping websites still does not use SSL during the checkout process.

(V) Encryption

So authentication checks to make sure that you are communicating with the actual person or machine that you are supposed to be communicating with, and not a hacker. However, what if the data that is being sent back and forth between the two parties is intercepted? If this happens we use a method called Encryption to shuffle and confuse the data so the hacker cannot make sense of the data. A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data. There are many differenet types of encryption and many different ways to implement it but for an E-commerce server you should make use of the Secure Shell or SSH method. It is a method that provides for an encrypted login connection to a server, for example, your Ecommerce Server. In this case, your customer's Username and Password, which would normally be sent as plain text over an insecure Internet connection, would be scrambled into an undecipherable format. This is saying when your customer types in their username and password to log on to the server, the SSH will make the username and password encrypted and scrambled so if a hacker does get a hold it they will not be able to figure out what the customer's username and password is. This prevents illegitimate users from accessing the E-commerce server.

(VI) Virtual Private Networks (VPNs)

Secure Sockets Layer (SSL) and Secure Shell (SSH) both encrypt your customer's Username/Password, Credit Card Number, Social Security Number, Home Address, etc. so that if a hacker gets a hold of this information then they will not be able to figure out or use the information. Another way to accomplish this task is to incorporate the use of a VPN or Virtual Private Network. Virtual Private

Networks are not just limited to encryption, but they make use of a feature called "tunneling" which adds another layer of protection. Tunneling is a very easy idea to grasp. To put it simply, the data packet that contains all of the information (username/password, email, social security number, etc.) from either the server or the customer and puts that data packet inside of another data packet to further hide and make the sensitive information even harder for a hacker to get into. The three main network protocols that are used for VPN's are Point To Point Tunneling Protocol(PPTP), Internet Protocol Security(IPsec), and Layer 2 Tunneling Protocol(L2TP). Point To Point Tunneling is used to access the Internet through a dial up modem. It also is a more secure form of Point To Point Protocol. Internet Protocol Security has different types and levels of security, such as ensuring the confidentiality and authenticity of the data packets. "This protocol makes use of advanced encryption techniques, such as Digital Signatures and Digital Certificates."(source 3) Layer 2 Tunneling Protocol, "The primary advantage of L2TP is that it can support other protocols." (source 3) This means that you can use L2TP with other VPN's that might be using a different protocol from the one that you are currently using. This can be a big advantage as not every protocol would make sense to use for every company, different companies will use different protocols depending on what their VPN must be able to accomplish. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Risk Management Approach

The term "when the dust settles" often is used when discussing e-commerce, and with good reason. The technology, the business models, and the value chain relationships are new and in many ways different from traditional business environments. The uncertainty concerns the character and degree of those differences. Nowhere is this truer than when discussing risks in e-commerce environments.

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals.

Principles of risk management

The International Organization for Standardization (ISO) identifies the following principles of risk management:

Risk management should:

- create value – resources expended to mitigate risk should be less than the consequence of inaction
- be an integral part of organizational processes

- be part of decision making process
- explicitly address uncertainty and assumptions
- be a systematic and structured process
- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement
- be continually or periodically re-assessed

Risks in E-Commerce

Risks categorized in three primary areas: information risks, technology risks, and business risks. Information risks stem from information published and contained in web sites and associated with the conduct of e-commerce. Peripheral to information risks are risks associated with misuse of information, such as violation of laws in the United States and other countries. Technology risks include risks involving hardware, software, telecommunications and databases. These risks include the consequences resulting from the misuse of technology or the use of inappropriate technologies required to address business needs. Business risks concern customer and supplier relationships, and risks associated with products and services marketed and distributed over the Internet. They also include risks associated with managerial aspects of the business including personnel and contractual relations.

Because e-commerce straddles many functional and technical areas, authors in many disciplines have identified e-commerce-related risks. Compiled a partial list of risks that appears below.

1. *Information Risk*
   - 1.1. Content on web page exposing web publisher to libel, defamation of character, slander
   - 1.2. Copyright infringement and invasion of privacy suits stemming from posted textual content
   - 1.3. Copyright infringement and invasion of privacy suits stemming from digital scanning and morphing
   - 1.4. Copyright, patent, or trade secret infringement violations by material used by web site developers
   - 1.5. After unauthorized access to a web site, online information about employees or customers is stolen, damaged or released without authorization

1.6. Electronic bulletin boards containing defamatory statements resulting in liability or embarrassment
1.7. Worldwide legal exposure resulting from use of creative material (e.g. names, likenesses) that violate laws of countries outside of the home country
1.8. Credit card information intercepted in transit is disclosed or used for fraudulent purposes
1.9. Information that has been changed or inserted in transmission is processed leading to erroneous results
1.10. Flight of intellectual property due to employees moving to competitors

Technology Risk

2.1. Negligent errors or omissions in software design
2.2. Unauthorized access to a web site,
2.3. Infecting a web site with computer viruses
2.4. Internet service provider (ISP) server crashes
2.5. Software error and omission risks causing unauthorized access
2.6. Software content risk that violates a copyright or is libelous.
2.7. Third party intercepts credit card information in transit causing breeches in security for online payments.
2.8. Intercepting and copying or changing non-credit card information during transmission
2.9. Insufficient bandwidth to handle traffic
2.10. Obsolete hardware or hardware lacking the capacity to process required traffic
2.11. Risk due to excessive ISP outages or poor performance
2.12. ISP phone numbers being busy
2.13. ISP or home-company servers being down
2.14. Scant technical infrastructure to manage cycle time to develop, present, and process web-based products
2.15. Risk of improperly integrating e-commerce system with internal databases
2.16. Risk of improperly integrating e-commerce system with internal operational processes
2.17. Risk due to poor web site design manifesting themselves in long response times
2.18. Inability of customer or supplier computers to handle graphical downloads

3. Business Risk

3.1. Web page content exposes web publisher to libel, defamation of character, slander
3.2. Electronic bulletin boards containing defamatory statements resulting in liability
3.3. Worldwide legal exposure resulting from use of information in violation of home-country laws
3.4. Using web sites to conduct illegal promotional games, such as a sweepstakes or contests
3.5. Risks related to payment to web site developers and disputes between developers and clients
3.6. Lack of maintenance on existing web pages
3.7. Impact on business due to intellectual property lost due to employees moving to competitors
3.8. Changes in supplier relationships re: data access, data ownership, distribution strategy, and marketing tactics
3.9. Changes in customer relationships re: data access, data ownership, distribution strategy, and marketing tactics
3.10. Products out-of-stock due to poor communication with operations
3.11. High shipping costs required for distribution
3.12. Inconvenient return policies — lack of coordination with physical system
3.13. Excessive dependence on ISP to support firm's business strategy
3.14. Inability to manage cycle time for developing, presenting, and processing web-based products
3.15. Risk due to unprotected domain names which are usurped by other organizations
3.16. Improperly integrating e-commerce systems with internal operational processes
3.17. Insufficient integration of e-commerce with supply chain channels

The above risks can lead to events resulting in the deliberate or inadvertent loss of assets. Deliberate loss of assets can result from disclosing information, fraud, or deliberate disruption of service. Inadvertent loss of assets can occur through inadvertent disruption of service, legal penalties due to disclosure of information, or direct or indirect losses due to lost business. As losses of these forms can occur in non-e-commerce environments, what are the similarities and differences between e-commerce and non-e-commerce risk environments?

Risk Comparison

To compare risks in electronic and non-e-commerce risks we postulate three risk categories:

Category A: Those risks that are essentially the same in either environment. For example, legal liability due to information improperly posted on a web page essentially is the same as legal liability due to information disseminated by printed or other electronic media.

Category B: Those risks that are essentially the same but that have unique dimensions dictated by e-commerce. For example, insufficient integration of e-commerce with supply chains might be an example of this risk.

Category C: Risks that is unique to e-commerce and which have never appeared before in other environments.

Analyzing the risks enumerated in the last section, yields a preponderance of risks falling in Category A. For example, our analysis, albeit subjective, indicates that all the Information risks — risks 1.1 through 1.10, Technology Risks 2.1 through 2.14, and Business Risks 3.1 through 3.14 all fall in this category. We conclude this because these risks — although they occur in e-commerce — essentially are the same risks that occur in other environments and have been managed in those environments.

There are several risks that we classify in Category B: Technology Risks 2.15 through 2.18 and Business Risks 3.15 through 3.17. For these, we conclude that although the risks are similar, the e-commerce environment is different enough to require unique treatment.

We found no risks in Category C — risks unique to e-commerce and not encountered elsewhere. Even those things that appear to be unique — for example illegal use of a domain name or risks associated with ISPs — have counterparts in use of logos or corporate names, and risks associated with organizations contracted for outsourcing data processing. Naturally we do not imply that the above list of risks exhaust all possibilities — certainly some may exist that fall in our Category B or even Category C. We do believe, however, that the majority of risks encountered in e-commerce environments have been encountered before and generally, are well understood if identified.

Can there be unique risks in electronic environments and if so, what are they? Although we have not identified any such risks here, we posit that they: 1) concern business issues that are unique to e-commerce and that are not found elsewhere; 2) involve technological attributes unique to e-commerce environments with no parallel issues found elsewhere; 3) impact risk in ways uniquely determined by characteristics of e-commerce.

Critical to managing e-commerce risks is a methodology that provides managers with the capability to identify assess and control risks on an ongoing basis. One proposed methodology that does this is a scenario-based methodology patterned on Information Security Management Planning (ISMP), a methodology implemented at a large money center bank to control information-based risks.

Methodology to Manage Risk

E-commerce Risk Management (ECRM), is based on scenario analysis and decision analysis, but differs from these techniques in several ways. First, by integrating business, operations, and systems managers into the risk analysis process, ECRM increases non-technical managers' ownership of the process and of the information-based risk issues. Second, ECRM is flexible enough to address issues specific to unique processing, geographic and organizational environments. Third, ECRM can be implemented at relatively low cost.

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

1. identify, characterize threats
2. assess the vulnerability of critical assets to specific threats
3. determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. identify ways to reduce those risks
5. prioritize risk reduction measures based on a strategy

ECRM can identify potential risk events in their early stages and by preventing their occurrence, lead to lower risk management costs. The actual risk management process consists of three phases:

Preliminary Risk Assessment

The Preliminary Risk Assessment (PRA) is a structured meeting between senior business, operations, marketing and systems managers. The PRA's purpose is to highlight for further analysis, the key risk issues and areas facing the business unit.

E-commerce risk is categorized in terms of risk target (where the risk occurs) and risk-type (Information Risk, Technology Risk, or Business Risk). The PRA focuses on outcomes based on errors, omissions, structural weaknesses, and deliberate acts.

The resulting grid generates "target-risk combinations". The risk assessment involves the senior business manager's providing a risk rating for each target-outcome combination, given existing controls. Highly rated risks (on a 1-5 scale) include an explanation for why the rating was applied.

Detailed Risk Assessment

In the Detailed Risk Assessment (DRA) the project team develops detailed risk scenarios for each highly rated PRA target-outcome combination. The bases for the DRA are scenarios based on the risks enumerated in above section. The DRA procedure is sequential includes:

- Meetings with managers from target areas to gain insights regarding risk scenarios;
- Brainstorming sessions and follow-up reviews to identify potential scenarios;
- Rating the scenarios regarding risk on a 1 to 5 scale;
- Identifying potential controls;
- Selecting controls to be implemented.

In this process, DRA risk ratings need not reflect the PRA target-risk combination rating. Cursory cost-benefit analysis often is sufficient to select or discard controls. Formal decision analysis is usually unnecessary and may be problematic.

The DRA's final step occurs when senior department and division managers review the scenarios and preliminary recommendations for final approval

Controls Implementation

In Controls Implementation the senior managers who participated in the PRA review the study findings and recommendations. Recommended controls frequently close security gaps for "high risk" scenarios, reduce risk exposure at minimal cost, or scrap obsolete controls which are holdovers from previous years and now address non-existent risks. Actually implementing the recommended controls is the methodology's final phase.

The growing importance of e-commerce in business requires controlling the associated risks. Fortunately, e-commerce-based risks are similar to those encountered in other business environments. Many of the requisite controls are extensions of controls for managing information systems risks.

Although one always hesitates to forecast too far into the future, if the past is any guide, many of the risks encountered in e-commerce environments will be people-based. It is management's ongoing responsibility to keep abreast to this situation and monitor, assess, and control risk in the burgeoning e-commerce environment.

Fifteen Steps to Managing E-Commerce Risk

The following steps have been identified as those that are most important to managing e-commerce risk.

E-COMMERCE START-UP	
1. **Know the risks and train your staff**	Your exposure to e-commerce risk depends on your business policies, operational practices, fraud prevention and detection tools, security controls, and the type of goods or services you provide. Your entire organization should have a thorough understanding of the risks associated with any Internet transaction and should be well-versed in your unique risk management approach.
2. **Select the right acquirer/ payment processor and service provider(s)**	If you have not yet launched an electronic storefront, you need to partner with a Visa acquirer/payment processor that can provide effective risk management support and demonstrate a thorough understanding of Internet fraud risk and liability. You also want to take a good, hard look at any service provider before you sign a contract. Bottom line? Does the service provider have what it takes to keep your cardholder data safe and minimize fraud losses?
WEBSITE UTILITY	
3. **Develop essential website content**	When designing your website, keep operational needs and risk factors foremost in your mind. Key areas to consider are privacy, reliability, refund policies, and customer service access.
4. **Focus on risk reduction**	Your sales order function can help you efficiently and securely address a number of risk concerns. You can capture essential Visa card and cardholder details by highlighting required transaction data fields and verifying the Visa card and customer data that you receive through the Internet.
FRAUD PREVENTION	
5. **Build internal fraud prevention**	By understanding the purchasing habits of your website visitors, you can protect your business from high-risk transactions. The profitability of your virtual storefront depends on the internal strategies and controls you use to minimize fraud. To avoid losses, you need to build a risk management infrastructure, robust internal fraud avoidance files, and intelligent transaction controls.
6. **Use Visa tools**	To reduce your exposure to e-commerce risk, you need to select and use the right combination of fraud prevention tools. Today, there are- a number of options available to help you differentiate between a good customer and an online thief. Key Visa tools include Address Verification Service (AVS)*, Card Verification Value 2 (CVV2)**, and Verified by Visa.
7. **Apply fraud screening**	Fraud-screening methods can help you minimize fraud for large-purchase amounts and for high-risk transactions. By screening online Visa card transactions carefully, you can avoid fraud activity before it results in a loss for your business.
8. **Implement Verified by Visa**	The tool Verified by Visa can create the most significant reduction in merchant risk exposure by increasing transaction security through cardholder authentication and by providing chargeback protection against fraud. E-commerce merchants who work with their acquirers to implement Verified by Visa are protected from certain fraud-related chargebacks on all Consumer and Commercial cards with limited exceptions. If applicable, E-commerce merchants may receive a reduced interchange rate.
9. **Protect your merchant account from intrusion**	Using sophisticated computers and high-tech smarts, criminals are gaining access to shopping cart and payment gateway processor systems, attacking vulnerable e-commerce merchant accounts, and making fraudulent merchant deposits. By taking proactive measures, you can effectively minimize this kind of cyber attack and its associated fraud risks.

10. Create a secure process for routing authorizations	Before you accept Visa cards for online payment, you must ensure that you have a secure and efficient process in place to submit authorization requests through the Internet.
11. Be prepared to handle transactions post-authorization	There are a number of steps you can take to deal effectively with approved and declined authorizations before you fulfill an order. The idea here is to apply appropriate actions that best serve your business and the customer.
CARDHOLDER INFORMATION SECURITY PROGRAM	
12. Safeguard cardholder data through PCI DSS compliance	The Payment Card Industry (PCI) Data Security Standard (DSS) provides e-commerce merchants with standards, procedures, and tools for data protection. For maximum security, you need reliable encryption capabilities for transaction data transmissions, effective internal controls to safeguard stored card and cardholder information, and a rigorous review of your security measures on a regular basis. PCI DSS compliance can help you protect the integrity of your operations and earn the trust of your customers.
CHARGEBACK AND LOSS RECOVERY	
13. Avoid unnecessary chargebacks and processing costs	For your business, a chargeback translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. It is important to carefully track and manage the chargebacks that you receive, take steps to avoid future chargebacks, and know your representment rights.
14. Use collection efforts to recover losses	You can often recover unwarranted chargeback losses through a well-thought-through collections system.
15. Monitor chargebacks	Merchants with chargeback monitoring mechanisms are in a better position to spot excessive chargeback activity, identify the causes, and proactively bring chargeback rates down by applying appropriate remedial actions.

Cyber law

Cyber Law is a rapidly evolving area of civil and criminal law as applicable to the use of computers, and activities performed and transactions conducted over internet and other networks. This area of law also deals with the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information. In the U.S. Cyber Law includes rules and regulations established by Congress, legislatures, courts, and international conventions to govern, prevent and resolve disputes that arise from the use of computers and the Internet.

Cyber law is a much newer phenomenon having emerged much after the onset of Internet. Internet grew in a completely unplanned and unregulated manner. Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. The growth rate of cyberspace has been enormous. Internet is growing rapidly . With the population of Internet doubling roughly every 100 days, Cyberspace is becoming the new preferred environment of the world. With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the

absolutely complex and newly emerging legal issues relating to cyberspace, CYBER LAW or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialized branch of law called cyber laws- laws of the internet and the world wide web. *Cyber laws that are in place to keep cybercrimes in check. In addition to cyber laws, it elaborates various IT Security measures that can be used to protect sensitive data against potential cyber threats.*

Cyber Law & IT Act Overview

(I) Cyberspace

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

(II) Cyber security

Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.

ISO 27001 (ISO27001) is the international Cybersecurity Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.

The Ministry of Communication and Information Technology under the government of India provides a strategy outline called the National Cybersecurity Policy. The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

(III) Cybersecurity Policy

The cybersecurity policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes "

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations

in designing suitable cybersecurity policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks.

It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Cyber Crime

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber crime. In a cyber crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber crime.

Cyber crimes can be basically divided into 3 major categories:

1. Cybercrimes against persons.
2. Cybercrimes against property.
3. Cybercrimes against government.

Cybercrimes against persons

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled. example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer

systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide.

Cybercrimes against all forms of property

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyberspy.

Cybercrimes against Government

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

In a report of expressindia. com, it was said that internet was becoming a boon for the terrorist organisations. According to Mr. A.K. Gupta, Deputy Director (Co-ordination), CBI, terrorist outfits are increasingly using internet to communicate and move funds. "Lashker-e-Toiba is collecting contributions online from its sympathisers all over the world. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathisers and also using the medium for intra-bank transfer of funds".

Objective

The recent Edward Snowden revelations on the US surveillance program PRISM have demonstrated how a legal entity network and computer system outside a particular jurisdiction is subject to surveillance without the knowledge of such legal entities. Cyber cases related to interception and snooping are increasing at an alarming rate. To curb such crimes, cyber laws are being amended quite regularly.

Emerging Trends of Cyber Law

Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods.

Some of the emerging trends of cyber law are listed below:

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
- Stakeholders of the mobile companies will call upon the governments of the world to reinforce cyber-legal systems and administrations to regulate the emerging mobile threats and crimes.

- The growing awareness on privacy is another upcoming trend. Google's chief internet expert Vint Cerf has stated that *privacy may actually be an anomaly.*
- **Cloud computing** is another major growing trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.
- The growth of **Bitcoins** and other virtual currency is yet another trend to watch out for. Bitcoin crimes are likely to multiply in the near future.
- The arrival and acceptance of data analytics, which is another major trend to be followed, requires that appropriate attention is given to issues concerning **Big Data**.

Create Awareness

While the U.S. government has declared October as the National Cybersecurity Awareness month, India is following the trend to implement some stringent awareness scheme for the general public.

The general public is partially aware of the crimes related to **virus transfer**. However, they are unaware of the bigger picture of the threats that could affect their cyber-lives. There is a huge lack of knowledge on e-commerce and online banking cyber-crimes among most of the internet users.

Be vigilant and follow the tips given below while you participate in online activities:

- Filter the visibility of personal information in social sites.
- Do not keep the "remember password" button active for any email address and passwords
- Make sure your online banking platform is secure.
- Keep a watchful eye while shopping online.
- Do not save passwords on mobile devices.
- Secure the login details for mobile devices and computers, etc.

Areas of Development

The "Cyberlaw Trends in India 2013" and "Cyber law Developments in India in 2014" are two prominent and trustworthy cyber-law related research works provided by Perry4Law Organization (P4LO) for the years 2013 and 2014.

There are some grave cyber law related issues that deserve immediate consideration by the government of India. The issues were put forward by the Indian cyber law roundup of 2014 provided by P4LO and Cyber Crimes Investigation Centre of India (CCICI). Following are some major issues "

- A better cyber law and effective cyber-crimes prevention strategy

- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legal issues of online payments
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard.

The transactions of cyber-insurance should be increased by the Indian insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

Why Cyberlaw in India ?

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

What is the importance of Cyberlaw ?

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Business Ethics

Business ethics (also corporate ethics) is a form of applied ethics or professional ethics that examines ethical principles and moral or ethical problems that arise in a business environment. It applies to all aspects of business conduct and is relevant to the conduct of individuals and entire organizations.

Business ethics refers to contemporary, standards or set of values that govern the actions and behaviour of an individual in the business organisation.

Business ethics, also called corporate ethics, is a form of applied ethics or professional ethics that examines the ethical and moral principles and problems that arise in a business environment. It can also be defined as the written and unwritten codes of principles and values, determined by an organization's culture, that govern decisions and actions within that organization. It applies to all aspects of business conduct on behalf of both individuals and the entire company. In the most basic terms, a definition for business ethics boils down to knowing the difference between right and wrong and choosing to do what is right.

Business ethics has normative and descriptive dimensions. As a corporate practice and a career specialization, the field is primarily normative. Academics attempting to understand business behavior employ descriptive methods. The range and quantity of business ethical issues reflects the interaction of profit-maximizing behavior with non-economic concerns. Interest in business ethics accelerated dramatically during the 1980s and 1990s, both within major corporations and within academia. For example, most major corporations today promote their commitment to non-economic values under headings such as ethics codes and social responsibility charters. Adam Smith said, "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices." Governments use laws and regulations to point business behavior in what they perceive to be beneficial directions. Ethics implicitly regulates areas and details of behavior that lie beyond governmental control. The emergence of large corporations with limited relationships and sensitivity to the communities in which they operate accelerated the development of formal ethics regimes.

Three levels of business ethics

In our mission to define business ethics, Johnson and Scholes provide a useful way of classifying the diverse elements therein:

- the **macro** level: the role of business in the national and international orgnisation of society the relative virtues of different political/social systems, such as free enterprise, centrally planned economies, etc., international relationships and the role of business on an international scale
- the **corporate** level: corporate social responsibility ethical issues facing individual corporate entities (private and public sector) when formulating and implementing strategies
- the **individual** level: the behaviour and actions of individuals within organisations

At the highest (macro) level, we ask the fundamental question of the role of business in society and what governance model works best to deliver the most benefits in a moral and responsible way. Morality itself is, of course a widely interpretable concept but for this purpose we will assume a broad understanding.

that of "proper behaviour" and "knowing the difference between right and wrong", without specifying what constitutes right and wrong. (This is a whole debate unto itself and subject to cultural and individual relativism). Suffice it to say here that morality sets the stage for ethics, and therefore the code of conduct by which business activity is carried out and allowed to be carried out by national and international rules and standards.

At the corporate level, the interpretation of those rules and standards is often what defines business ethics, affected by the specific circumstances and socio-cultural context in which the business or public sector organisation is operating. While all corporate entities in theory are directly influenced by personal morality and ethics, in practice there is often a gap between the behaviour of individuals within the working environment and outside it. This, we would argue, is one of the major factors leading to mistrust of big business, where the separation of ownership and management is greatest, and so open to abuse. Even if directors/senior managers are not acting unethically, it is likely they would act differently if the money and the company about which they are making decisions were their own. (There are obvious exceptions as with any generalisation.)

At the individual level, this separation creates a distinct ethical model - business ethics - which, depending on factors like personality, peer pressure and the socio-political environment, can be closer or further away from the individuals own moral/ethical code of conduct. With limited liability meaning individuals are protected this can affect smaller businesses too as the consequences of one's actions has a greatly reduced impact on personal circumstances. Clearly, every corporate entity is directly affected by the individual's moral and ethical stance - and any difference between business and personal ethics is itself arguably an indictment of that individual stance as it implies some level of double standards.

Measuring business ethics

So we would define business ethics not only as subscribing to the principles of responsible business, but actually having effective controls - including collecting primary research data - on how each stakeholder group perceives the company's performance on a range of issues which constitute business ethics. As we have said, this presents a challenge for business if people define business ethics differently. The way round this is to use proxies - observations and opinions on manifestations of good ethical performance.

Managing Ethics in the Workplace

Managing Ethics Programs in the Workplace

Organizations can manage ethics in their workplaces by establishing an ethics management program. Brian Schrag, Executive Secretary of the Association for Practical and Professional Ethics, clarifies. "Typically, ethics programs convey corporate values, often using codes and policies to guide decisions and behavior,

and can include extensive training and evaluating, depending on the organization. They provide guidance in ethical dilemmas." Rarely are two programs alike.

"All organizations have ethics programs, but most do not know that they do," wrote business ethics professor Stephen Brenner in the Journal of Business Ethics "A corporate ethics program is made up of values, policies and activities which impact the propriety of organization behaviors."

Developing Codes of Ethics

According to Wallace, "A credo generally describes the highest values to which the company aspires to operate. It contains the 'thou shalts.' A code of ethics specifies the ethical rules of operation. It's the 'thou shalt nots.'" In the latter 1980s, The Conference Board, a leading business membership organization, found that 76% of corporations surveyed had codes of ethics.

Some business ethicists disagree that codes have any value. Usually they explain that too much focus is put on the codes themselves, and that codes themselves are not influential in managing ethics in the workplace. Many ethicists note that it's the developing and continuing dialogue around the code's values that is most important.

Developing Codes of Conduct

If your organization is quite large, e.g., includes several large programs or departments, you may want to develop an overall corporate code of ethics and then a separate code to guide each of your programs or departments. Codes should not be developed out of the Human Resource or Legal departments alone, as is too often done. Codes are insufficient if intended only to ensure that policies are legal. All staff must see the ethics program being driven by top management.

Note that codes of ethics and codes of conduct may be the same in some organizations, depending on the organization's culture and operations and on the ultimate level of specificity in the code(s).

Resolving Ethical Dilemmas and Making Ethical Decisions

Perhaps too often, business ethics is portrayed as a matter of resolving conflicts in which one option appears to be the clear choice. For example, case studies are often presented in which an employee is faced with whether or not to lie, steal, cheat, abuse another, break terms of a contract, etc. However, ethical dilemmas faced by managers are often more real-to-life and highly complex with no clear guidelines, whether in law or often in religion.

As noted earlier in this document, Doug Wallace, Twin Cities-based consultant, explains that one knows when they have a significant ethical conflict when there is presence of a) significant value conflicts among differing interests, b) real alternatives that are equality justifiable, and c) significant consequences on "stakeholders" in the situation. An ethical dilemma exists when one is faced with having to make a choice among these alternatives.

Assessing and Cultivating Ethical Culture

Culture is comprised of the values, norms, folkways and behaviors of an organization. Ethics is about moral values, or values regarding right and wrong. Therefore, cultural assessments can be extremely valuable when assessing the moral values in an organization.

Ethics Training

The ethics program is essentially useless unless all staff members are trained about what it is, how it works and their roles in it. The nature of the system may invite suspicion if not handled openly and honestly. In addition, no matter how fair and up-to-date is a set of policies, the legal system will often interpret employee behavior (rather than written policies) as de facto policy. Therefore, all staff must be aware of and act in full accordance with policies and procedures (this is true, whether policies and procedures are for ethics programs or personnel management). This full accordance requires training about policies and procedures.

Questions

Very Short Questions :

1. What is Zombies ?
2. What is ping of Death ?
3. VPN Stand for ?
4. What is SSL ?
5. What is SSH ?
6. What about ECRM ?
7. What is PRA and DRA ?

Short Questions :

1. What is Malware ?
2. What do you mean by Macro Vireses ?
3. What is worms ?
4. What is the difference between Spy ware and Adwae ?
5. What is IP Spacefing and Part Scanning ?
6. Explain Business Risk?
7. What is the importance of cyber law ?
8. Explain level of business ethics in brief..

Long Question :

1. What do you mean by Maluare ? Explain its characteristics.
2. Write a short note on virus and Explain every three type of virous.
3. What do you mean by Transmission Threats discuss indetail.
4. Explain-
   (a) Data packet Sniffing
   (b) IP Spaofing
   (c) Part Scanning
   (d) Trupdoors/Backdoors
5. Explain Fivewalls
6. What do you mean by Risk Management ? Explain its Principles.
7. Explain alltype of Risk in E-commerce ?
8. Write a short note on Cyber Law ?
9. What is Business ethics ? Explain the level of Business ethics ?

□□□