ARRAY Logo

icon

Preventing Technology Based Bank Frauds

By V.Radha, Faculty, IDRBT

Web:http://www.idrbt.ac.in
Email: vradha@idrbt.ac.in

Ms.V.Radha, is faculty at IDRBT and is involved in various activities of the Institute like - teaching Mtech students, co-coordinating programs for Bankers, Implementing applications etc. Prior to joining IDRBT, she has worked in UNDP projects of IGNCA, New Delhi and LIBSYS.

She is currently pursuing her Ph.D in Computer Science from the University of Hyderabad. Her areas of interest include Computer Applications, Databases, Networks, Communications and Internet

By Ved P. Gulati, Director, IDRBT

Web:http://www.idrbt.ac.in
Email: vpgulati@idrbt.ac.in

Dr. V.P. Gulati is Director, Institute for Development and Research in Banking Technology (IDRBT), Hyderabad. In a career spanning over two decades of intensive academic and research activities, he has been in the forefront of leveraging IT for operational excellence in the domain of banking and financial services. Equipped with academic credentials from the IITs, Dr. Gulati is an ardent ally of cutting edge technologies, and is associated with eminent institutes and banks, is a member of many national level committees and advisory boards, and author of a number of refereed papers and publications.

Dr. Gulati has been instrumental in the development of IDRBT from its nascent stage to an Institution of Excellence and Expertise. He spearheads the Institute's Research and Development Initiatives, and provides strategic direction in offering Executive Development Programmes, Academic Programmes like M.Tech. and Ph.D., hosting seminars and conferences on contemporary issues, and providing advisory services to the Banking sector.

Abstract

New technology always brought some more fraudulent criminal activities developed around these technologies. Ex: Photocopiers, fax machines, credit cards, and mobile phones, ATMs, PCs and now Internet. By the time the regulatory bodies, law enforcement agencies etc take preventive measures to cope up with the present environment and it gets stabilized, either the environment itself changes or some more new elements like new technology emerges making the criminals find a new home and commit fraud. So prevention is basically a cycle of monitor, analyse, detect, act and protect.

In this paper we discuss about the technology based opportunities that thieves take advantage and its prevention and how to build future technology based banking services that can limit the

frauds.

1. Introduction:

Thieves are not born, but made out of opportunities. All the major operational areas in banking represent a good opportunity for fraudsters. Majority of the fraud incidents being reported is under deposit, loan and inter-branch accounting transactions, including remittances. The advent of computerization in banks brought new technology based frauds, when committed successfully, would be difficult to track down and can multiply the financial losses of banks to unimaginable levels. A careless pressing of a button, resulted in 100 crores loss to a stockbroker in BSE, as he couldn't undo his wrong quote (Business Line). Preventive fraud management is therefore far superior to post fraud containment or recovery of losses.

Prevention is basically to limit/eliminate the opportunities so that thieves are not born and take away money by indulging into frauds. It is very difficult to look into all permutations and combinations of opportunities that thieves take advantage and prevent them so that they never surface. Only effective continuous monitoring and analysis of fraudulent activities help understand the reason behind a fraud and then take counter preventive measures.

New technology always brought some more fraudulent criminal activities developed around these technologies. Ex: Photocopiers, fax machines, credit cards, and mobile phones, ATMs, PCs and now Internet. By the time the regulatory bodies, law enforcement agencies etc take preventive measures to cope up with the present environment and it gets stabilized, either the environment itself changes or some more new elements like new technology emerges making the criminals find a new home and commit fraud. So prevention is basically a cycle of monitor, analyse, detect, act and protect.

2. Technology in Banking - The Past

Most Public Sector Banks started computerization of their business, particularly branch automation based on the Ranga Rajan committee report in the eighties. Those days the main aim was to convert the laborious manual process into simple automated process with out re-engineering any business process. The CVC (Central Vigilance Commision) strongly believed (particularly after Harshad Mehta's Scam) that frauds can take place at a higher rate due to slow and delayed manual processes and forced Banks to computerize their branches with no one actually guiding or monitoring the whole computerization in Banks. Banks went in their own way computerizing their branches, without having any holistic integrated approach not only among banks but also in their own bank with in their branches.

This led to isolated applications at branch levels, and almost every PSB (Public Sector Bank) ended up with different flavors of branch automation from different vendors mainly due to 2 reasons.

a. Software Vendor of Regional choice as maintenance charges from local vendors would be cheaper
b. No single vendor has over all presence across India.

1.1 Problems with this technology:

- Islands of applications in the branches of a bank, with dissimilar computers, operating systems and application packages. There's no integration of such application and hence forcing the manual intervention.
- Due to various flavors of hardware and software, no data integrity could be maintained even though the application was for the same business purpose. Ex: No one could see a unified picture of overall deposits, loans customer information etc of the whole Bank.
- Due to dissimilar application packages, Inter branch reconciliation and communication was not possible. Even if it was made possible, it was not straight through.

- Still some banks are continuing with this technology which is very out dated
- Not able to trust vendors, banks relied on half vendor based software and half in-house software. They couldn't integrate the two, without some manual intervention.

Due to the above problems, banks are still dependent on manual procedures only. More than 50% of the process of generating MIS from the branches and send to their Central Office required manual intervention.

This technology helped banks, only to lessen some burden on back office. It couldn't achieve

- Better monitoring control
- Better decision making
- Faster service delivery
- Better performance
- New products or services etc

Instead of alleviating the threats posed by manual banking, it actually increased them further, leaving lot of confusion on whom to make accountable, the computer or the computer operator.

Some of the new fraud techniques that surfaced due to computerization

- Intentionally writing programs to siphon off the funds
- Illegal transactions between accounts
- Wrong interest calculations (Deccan Chronicle 15/12/2k2)

Today, many PSBs have computerized branches, but this computerization helped neither banks nor the customers as expected.

3. Technology in Banking - The Present

Introduction of foreign and private banks coupled with Information Technology and Global computer Networks, posed a big threat to Public Sector Banks. Right now, banks with no option left, but to turn to technology in order to compete (even to survive) with foreign and private sector banks.

Not satisfied with the already existing technology, banks now have decided to re-look into the whole technology adoption with fresh management goals and commitment. Many of them decided to phase out the old branch automation software in phases, with high aim of satisfying the customer and integrate the whole back office and generate MIS online.

With this aim, banks are now setting up their networks so that they can have a overall bank view instead of just a branch view from all the angles of process, control, monitor, decide and act. They also chalked out plans on how to deploy their applications on this network infrastructure.

At present the foreign and private sector banks are in a position to offer the banking services through many delivery channels and integrate both front-office and back-office operations.
The delivery channels

- Internet Banking
- Phone Banking
- ATM
- ABB

Since it's the customer who is the king in any business, the PSBs are confused in deciding which one of the following methods suits them best

- To satisfy the customer first, just add some additional layer on the existing technology and set up proper back-office systems later
- To revamp everything – right from branch operations, to a new technology.

Many banks have taken the very first approach, ie some how come to forefront of the technology by offering all kinds of services on every possible delivery channel.

This requires lot of technology awareness, expertise etc with in a bank, without which the bank can become a prey of new technology based frauds.

4. Frauds in Present Technology Environment

With banks deciding on setting up networks and computerize the whole banking process, to offer their services on multiple channels, they now face risks both from inside and outside. This section describes the kind of frauds that can happen in this environment.
Some more avenues for frauds in this emerging banking scenario

- **Mail Spoofing** – E-Mail Forgery: sending wrong information to bank customers as if its from authentic bank sources
- **Web Spoofing** – Web Site Forgery: Diverting the customers of a bank to an exactly duplicated forged web site and impersonating those customers on real bank site
- **Attacking the User Computer**: To take control of that machine
- **Attacking a Bank's Server**: To take control of that machine
- **Media Tapping** – recording the whole transactions of a bank, or customer etc and replaying the same for their advantage
- **Denying Service**: Though the server is available, making it not able to render service, by poisoning the Network Infrastructure

4.1 Mail Spoofing – E-Mail Forgery:

Kola Mohan's Case: (Taken from Rediff Web site)
This is the first cyber crime in Andhra Pradesh. Kola Mohan, was able to convince several gullible money lenders, top banks and the state's ruling Telugu Desam party that he had won the Euro Lottery and that he was awaiting to complete a few formalities before the millions were transferred to his account in India.
He set the ball rolling in November 1998, just a few months after he actually picked up an Euro Lottery ticket in London, when a prominent Telugu daily received an e-mail (sent by Kola Mohan himself) saying that a Telugu man had won the multi-million dollar Euro lottery but no one had taken notice of this great achievement.
The newspaper promptly published a report and followed it up with an interview without making any attempt to contact any Euro Lottery representative. Other newspapers soon picked up the story and Kola Mohan became a celebrity overnight.
Now it was time to put into motion the second part of his plan. He began calling up money lenders seeking short-term loans which of course he would pay back as soon his "money arrived from London where it was deposited in a bank."
Kola Mohan's dream run continued till creditors began putting pressure on him. By October 1999, the word was out that his claims about his Euro Lottery win were fake.
But Kola Mohan was not going to give up so easily. He showed his creditors some documents issued by the Midland Bank, Sheffield, UK, where he claimed he had made some investments that were due to mature on November 17, 1999. Around the same time, a Andhra Bank cheque of Rs 1.73 million issued by Kola Mohan also bounced. Kola Mohan had pledged with the bank the copy of a bond certificate purportedly issued by Midland Bank Trust Company Limited, London stating that a term deposit of 12.5 million pounds was held in his name.

4.1.1 Cause of the above fraud:

1. **Source Address Authenticity never verified**

The e-mail system was developed trying to imitate the postal mail. Just like in postal mail, the "From Address" authenticity was never verified. Though the new mail systems have that capacity, no one can actually stop any one from setting up a mail server that has this flaw. Using this server, anyone can forge a mail posing as an authentic source.

2. **Reply can be sent to a different mail address as preferred by the sender instead of the Source Address**

Another major flaw in e-mail system is that the sender can always set on which e-mail address to get the reply to his mail. Ie the forger can send a mail with the forged source e-mail address; can set its reply address as his own e-mail address, so that the replies reach his actual e-mail address instead of the forged e-mail address.

Due to the above flaws, a forger can easily pose as any well-known personality, without the knowledge of that individual. The receiver always thinks that the mails were from the said address, and his replies go actually to the forger than to the real person.

4.2 Web Spoofing – Web Site Forgery

Hackers find new way to bilk eBay users (Source:news.com)

Someone other than Gloria Geary had access to the Washington artist's eBay account.

Using Geary's user ID, the person set up an auction for an Intel Pentium computer chip. Not only that, but the person changed Geary's password so she could no longer access her own account--or cancel the bogus auction.

Geary, who discovered the auction Friday, was able to convince eBay to pull down the auction over the weekend, but not before suffering through a stressful day of worrying about how the auction would affect her legitimate listings.

"I felt totally violated. I was shaking," Geary said. "It's appalling the ease at which they totally took over my account."

Geary is only the latest victim of an increasingly popular scam on eBay. Since January, the company has received a growing number of complaints from people such as Geary who say their accounts have been taken over and used to set up fraudulent auctions. The scam artists make a quick buck, then leave the legitimate eBay users to deal with the furor from bilked bidders.

The scam involved e-mails that asked recipients to log on to a Florida-based Web site, ebayupdates.com, and re-enter financial data for eBay, said Dean White, the Asia-Pacific "Once you've got the credit card information, you can use it for everything," White said.

The fake site sported the eBay logo and colors but did not appear to have any connection with California-based eBay.

In a similar fashion, even the bank sites can be forged. The customers of the bank can be lured to log on to fake web site, which exactly looks and behaves as the original, at least till it captures the customers' username and password. These forged web site owners, pose as the real customers of the bank and log on to the real site and do transactions with the already captured username and password. The bad part of the whole issue is that the customers do not have any means of proving that it was not they who did those transactions, but some unknown persons. This kind of fraud has been increasing on Internet, to steal username, passwords and credit card info etc.

4.2.1 Cause of the above fraud:

1. Users actually can't understand how an URL (Universal Resource Locator, that every one type in a browser after http://) should be interpreted. They just see the first few strings of the URL and if it just includes the web site name they want to access, they are satisfied. For Ex: Take these 2 URL
    a. http://secure.bankname.com/mutualfnd/mutualfunds.asp
    b. http://secure.bankname.com:any?@202154156/mutualfnd/mutualfunds.asp

    It would be very difficult for a normal user to understand the difference between these two URLs. While the first one takes him to the right bank site, the other one can take him to a forged site, in which he can reveal his username and password.
2. The URL can be circulated to all users using the E-mail forgery mechanisms described earlier. Instead of typing the whole URL or going from the homepage of the original web site, the user just clicks the hyperlink given in the e-mail.

4.3 Attacking the users' computer

In this type, the fraudster implants a virus, Trojan horse into the victim's machine, and using that program he monitors all transactions, steals vital data like username & password and then impersonates the victim. The virus, Trojan horse can be implanted into the victim's machine by using numerous methods like e-mails, IRC – Internet Relay Chat, fake web sites.

4.3.1 Causes for the above crime:

Though early e-mail software allowed only messages in text, due to demand from users, the software is made more intelligent in that it can now accept any kind of data, audio, video and executable files; and execute the same just by a click of button.

The same is true with Web Browsers and IRC software. These are capable of downloading any kind of executable and run the same instantly.

4.4 Attacking the Banks' Servers

In all the above cases, the fraudster didn't touch the technology infrastructure of the bank and so bank is as such not responsible for its user getting impersonated. However, in this case, the fraudster directly takes control of the bank's server; does transactions impersonating many customers (even the internal staff can be impersonated now) of the bank; and even can delete all the transaction log files of him visiting the bank's site, such that he can't be traced back.

4.4.1 Causes for the above fraud:

Almost all-general purpose software like Mail Server, Web server, Operating System are plagued by Buffer-over-flow attacks that stem from bad programming practices. These buffer-over-flow flaws in software allow the fraudster execute any command of his choice on the server, by just inputting the command instead of inputting the data - like name, password etc.

4.5 Media Tapping

Media tapping involves the fraudster collect all the digital bits that travel across the physical communication wire. Only those, who have physical access to the media, can commit this kind of crime.

4.5.1 Causes for the above crime

- Media Properties like broadcast
- The network protocols like TCP/IP, which basically do not employ any security mechanism by default; and allow information flow in clear text through out the network

4.6 Denying service from Banks' servers

The aim of these kinds of frauds is to cause inconvenience to the bank by making it disrepute, and take away its customers. The customer just can't access the bank's services.

4.6.1 Causes of the above fraud:

1. **The network protocol nature**

   The TCP/IP protocol, the computer communication language, specifies how a particular task (ex: call initiation) should be performed. But it doesn't specify, how to react in case of exceptions. Different operating systems implemented these exceptions in different manners and this allowed fraudster to take advantage.

2. **Router poisoning**

   Routers are like traffic junctions that lead customers to different parts of the network. Just like the signboards at traffic junctions that help motorists find their way, each router keeps routing information (called routing tables) that helps the packets reach their destination. Any one can dupe the router to change its routing table.

3. **DNS spoofing**

   Computers communicate through IP numbers, which are unique numbers just like telephone numbers. Unlike telephone numbers, these numbers are difficult to remember. Since it's actually the user who instructs his computer to communicate with the other, one more addressing scheme was devised ie computer/host name. So, when the user types the computer name, the name is converted to IP number and using that IP, the

communication starts. The service that does this translation is called DNS – Domain Name System Service. If this DNS service, misbehaves, the user would be diverted to some other server instead of the original server.

4.6.2 A Case: In Hyderabad, www.vsnlinternet.com is diverted to a porn site

Some of our users who automatically renew their VSNL accounts through HDFC BANK site have brought this case to our notice. So, whenever a user was trying to renew his VSNL account, from the facility offered by HDFC, the users were being diverted to a porn site. After, verifications, the author came to know that it was because of a poisoned DNS server of VSNL. The office's DNS server, which contacts this DNS server, also got poisoned and it too was diverting all users. Once the office's DNS server is made to point to another DNS server of VSNL, it started working properly. The VSNL authorities were informed of the same.

5 Technology in Banking: The future

In the whole above discussion, the bank couldn't utilize any extra benefit from the technology apart from being able to conduct its own business on different channels; at any time and offering more convenience to customer. Instead, its now exposed to many more threats. Its old fashioned frauds in loan and deposits areas couldn't be circumvented with all these technology initiatives. Frauds that involve loan defaulters, same property given as mortgage at different banks, loans to fake companies etc couldn't be avoided, as there's no way for the bank to check the authenticity of the information. This means, that we have to look from a different perspective altogether from every angle instead of just looking at Bank automation and how to improve Bank Service Delivery.

Many frauds are due to forged documents, forged identity, false information etc. Not only just Banks, but also almost all the organizations on which the Banks depend for authentic information should be computerized, networked and their software applications should share the information online in secure, authentic manner. Unless this happens, whichever technology the banks adopt, whatever control measures they take, frauds do take place.

5.1 Web Services/Straight Through Processing:

Web Services technology allows, the servers disseminate the information in structured form using XML (extensible Mark Up Language), not only to individual operators, but also to other application servers, irrespective of which software, hardware and database they use. Using this, the other remote applications can easily avail that information to take any decision or process their own business transactions. For Ex: RBI now, allows one to verify whether an individual or a company has defaulted or has become NPA – Non Performing Asset. But to check this, one has to visit RBI web site and query their database manually. It would be difficult for a bank employee to do that, before he sanctions a loan. Similarly, Registrar of Companies database is made available on CD – Compact Disk by NIC – National Informatics Center. But even this expects one to check individually from that CD only, for a company's information. Same is the case with Land Registration Authority. All have computerized their environments, but they are independent islands. Unless all these computerized applications talk to each other online, no one can actually use it well for better purpose.

For this to happen, RBI, Registrar of Companies, Land Registration database etc have to set up web services and allow other applications utilize the same. In this case, whether an individual operator verifies the information or not, the loan sanction application verifies the same online and alerts him, in a platform independent way – ie all these organizations can set up their services on platforms of their choice but still able to communicate. At IDRBT, a prototype of how these applications interact has been developed. In our prototype these 3 applications ie RBI, Company Registrar and Land Registrar are hosted on different platforms and the bank loan processing application is written in Visual Basic.

5.2 Application: Online Borrower Verification

The scope of this application has been limited only to verify online the authenticity of the borrower, his company and the property he mortgages while processing a loan form. There are three checks and one direct update of the "Property Record" from the bank into the database of "Land Registration Authority".

Company Registration Check:

The *Company Code* is a unique id that identifies a company that is registered with the 'Registrar of Companies'. Once the bank operator enters this code, the application contacts the "Registrar of Companies" database online and displays the entire information of the same, if that code exists. By looking at the information on screen and the information provided to him, the operator can decide on the information. Otherwise, if the code and company doesn't exist at all, the application does not allow any further actions.

Defaulters Check:

In case the company is a defaulter, the complete details of where it has defaulted, amount, etc are returned, as the application directly contacts the "RBI Defaulters Database".
The application also allows search by bank. This requires the *bank code* as the input, and all the companies that have defaulted from the bank are displayed.

Land property Check:

This check is carried out only if the above 2 checks are successful. This check involves entering the *Asset ID* (which is unique), which in turn returns the current *status* of the asset (mortgaged/not-mortgaged).
The details of the asset (like the Owner, Date of Purchase, Present worth, etc) are displayed.

The application does not allow the user to mortgage an already mortgaged asset, by displaying a message that 'the asset cannot be mortgaged'.

In case, the third check is also successful, the application asks for confirmation from the user about mortgaging the asset. If the borrower accepts to mortgaging his asset, the application updates the new status (i.e. mortgaged) in the database of "Land Registration Authority".

Though, it looked very simple in this prototype, it actually requires lot of back ground work from all the organizations. It is very difficult for all these organizations (not only the one mentioned in our prototype, but also others like Insurance, Health Department, Passport Office, IncomeTax etc) to communicate with each other and deploy these services. Instead a National Body should decide how all these organizations could share which kind of information at what time etc.

6. Prevention

In this section let us discuss the prevention mechanisms. In all the sections we discussed the technology and the frauds that can occur due to that. A close observation reveals that all frauds happen due to impersonation, sniffing information on its travel and hacking into the computer. The impersonation can be for an individual, a web site, a computer, a router etc. The frauds due to impersonation, sniffing can be minimized by adopting PKI – Public Key Infrastructure. Frauds due to hacking and not able to deploy PKI, etc can be minimized by firewalls, IDS – Intrusion Detection System.

6.1 Security Requirements

The following are the basic security requirements in a remote communication.
Authenticity: In a networked environment, asserting the source of the message has always been of importance. Particularly due to many TCP/IP and Internet applications flaws, the problems of Web Spoofing (forged web sites), IP spoofing (forged IP addresses), DNS Spoofing (forged

Domain Names) are of major concern.
Non-Repudiation: The recipient of the message should be in a position to prove that he received the message only from the said sender mentioned in the message, and sender can't deny that.
Integrity: Ensures that the message hasn't been tampered in transit.
Confidentiality: Ensures that only the said recipient of the message can read, but no one else.

Authorization: Able to confirm that the sender has the right to send the message.

6.2 Public Key Infrastructure
Public Key Infrastructure assures "Confidentiality", "Authenticity" and "Integrity" of the information which 2 or more members exchange. The PKI relies on Public Key Cryptography and hashing techniques.
Public Key Cryptography: The Development of Public Key Cryptography is nothing short of a revolution in the history of Cryptography. Public Key Cryptography is asymmetric, involving the use of two separate related keys – Public Key to Encrypt; and the Private Key to decrypt with either of the two related keys being used to encrypt, and the other being used for decryption.
Its advantage is that Key Management becomes much easier. If A has to communicate with 10 persons, he need not share 10 different secret keys as in the earlier case. Instead, he just has to share his Public Key, irrespective of the number of people he communicates with. But it is computationally inefficient in terms of speed, and moreover, it also involves a trusted third party, commonly known as Certification Authority.
Hashing Techniques: PKI uses Hashing techniques to ensure the integrity of the message. A hash function generates fixed size hash code for a given message, called message digest. The main characteristics of one-way hash functions are as follows:

- No two messages can have the same message digest
- The message digest is a function of all bits in the message and any change in the data will result in a change in the message digest
- It is not feasible to compute the original message from the message digest.

Using both Public Key Cryptography and hashing techniques, the security criteria "Confidentiality", "Authenticity", "Non-Repudiation" and "Integrity" of the message can be met.
If the Public Key has been used for Encryption, only the one who has its corresponding Private Key can read the message and hence assures confidentiality.
If the Private Key has been used for Encryption, only the one who has the Private Key must have sent the message, and hence assures the authenticity and non-repudiation of the message.
Sender "A" to send a confidential message to "B", he does

- Encrypts the message with B's Public Key
- Computes the hash of the message
- Encrypts this hash (also called signing) with his own private key
- Sends all these three components to B

At the receiving end, B does

- Decrypts the hash with the Public Key of B and gets the hash sent by A
- Decrypts the message with his own Private Key
- Computes the hash on his own of this message
- Compares the hash sent by A and the one he computed
- If they match, the message has met all security criteria including integrity, if not the message should be discarded

It's actually the software, which does all this at both the places; individuals keep only Private Keys secret.
Digital Certificates: Users of Public Key based systems must be confident that at any time they rely on a public key, the subject that they are communicating with owns the associated private key, and this applies irrespective of whether an encryption or digital signature mechanism is used. This confidence is obtained through the use of Digital Certificates, which are data structures that bind Public Key values to subjects. The binding is achieved by having a trusted CA verify the subject's identity and digitally sign each Public Key along with many user credentials. So instead

of a Public Key, one has to distribute his digital certificate to the public.

Certification Authority: An authority trusted by many users to issue Digital Certificates and to manage the PKI.

PKI Applications:

PKI can be utilized at all levels like

- Communication among users by issuing digital certificates to users
- Communication among servers and users by issuing digital certificates to servers and users – (SSL uses this mechanism)
- Communication among network devices like routers, switches, computers etc by issuing digital certificates to these devices (IPSec uses this mechanism)

6.3 PKI and Present Deployment:

At present PKI is being used very well, for closed corporate business. However, across different networks or Internet, it still has to take a long way. On Internet, for 2 purposes PKI is being used extensively.

1. **Secure Communication between Customer and Service**

   In present deployment of PKI, it's able to secure the communication so that no one can sniff the information passing on wire. Digital Certificates are issued only to servers, ie clients can authenticate the servers, but the servers authenticate clients using "Usernames" and "Passwords".

   In case of web based transactions, SSL (Secure Socket Layer – uses PKI) allows the client to interact with server in a secure fashion, but it's the web browser who authenticates or rather trusts the server by using the trusted root certificates that already come with web browsers. Here the user may or may not be aware of what these certificates are and who has put them in his browser or machine etc. In a way its like web browser software, which is taking decision on behalf of user.

   The current SSL and Internet Security architecture doesn't provide any non-repudiation mechanism, as what happens at the server or service while transacting is unknown to anyone. SSL only protects the channel communication by encrypting the data before transfer. Once its transferred to the server, the data would be in the hands of the service (or the service provider), which can tamper the information or misuse.

2. **Software Authentication**

   In many frauds, it is the software (virus, Trojan) that misleads/impersonates the customer. So to protect the customer from this malicious software, the new concept of authenticating the publisher of the software is gaining importance. In this method, the publisher would sign the software before dispatching it to users, and the user's machine checks the authenticity of the publisher and alerts the user accordingly.

Fraudsters can cheat even after deploying PKI

Even after all these efforts, fraudsters can still cheat the users, due to the following reasons.

- The browsers alert the user, only if they don't find the CA certificate that issued Digital Certificate to the server/publisher. However, it still allows the user to go ahead with further communication.
- Anyone can set up a CA, and issue digital certificate to themselves and make the browsers trust them.

6.3 How to Strengthen the PKI further

As a technology PKI is superior. Only due to implementation problem, one couldn't achieve full security. All individual customers also should get Digital Certificates. Even servers should

authenticate the customer using PKI and then only render the service, instead of relying on "User Name and Password". Instead of CA certificates, installed automatically in browser software by Microsoft or Netscape, an Indian Authority must have control on which CA certificates must reside in Indian Consumers' Browsers and which should not.

6.4 Firewall and IDS – Intrusion Detection System

The underlying TCP/IP communication protocol that is basis for computer networks has no concepts of security, privacy, integrity built into it. The old TCP/IP and it's associated application protocols are now being strengthened by new protocols like IPSec at the network layer, SSL at session level and 'Digital Certificates to users' at application level. Use all these mechanisms where ever possible.

Since it is not possible to use all these mechanisms at all locations due to various reasons like incompatibility between products, versions and implementations, one has to look at solutions like Firewall and IDS which give a over all security at the network perimeter, closing the security holes of desktops, servers etc by restricting access into the network. A firewall acts as a super cop inspecting the traffic between networks. While this method can secure corporate networks from being hacked, personal home computers can secure themselves by installing Personal Firewalls and IDS.

7. Need for National Organizations for Financial Sector

From the above discussions, it is clear that 100% preventions are impossible. Internet and its technology with in Intranets grew to such an extent that it is highly difficult to close the holes that it left.

There is a need for an authority, which authorizes any electronic services by specifying norms, standards and business practices for conducting business online. No one should set up a service or server for business purposes, without taking permission from this authority, just like Registrar of Companies. Separate organizations can be thought of, for different functionalities like – Certifying Authority, Security Audit, Incident Response, Information Sharing, Consultancy and Training etc, which help the banks in their ongoing efforts to adopt the technology and live with the technology.

The software and hardware used by (business) service provider should be verified by the authority and the integration of software and hardware devices through the APIs provided by both the sides, should be checked and disclosed, in such a way that the service provider can no way tamper with the information of the user while rendering the service. This is needed not only to protect the privacy of the user, but also to help fair on-line transactions without allowing any fraud to take place.