IDRBT
The Think - tank for Banking Technology

FAST FORWARD

A Quarterly Newsletter
from
Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)
Hyderabad - 500 057, INDIA.

Vol : 4 January 2001 No : 1

Conference of Chiefs of Public Sector Banks and Heads of Dept. of I.T on INFINET and Applications

On 14th December, 2000, the conference of Chiefs of Public Sector Banks and Heads of I.T. on 'INFINET and Applications' was held at the Institute. Shri. S.P. Talwar, Deputy Governor, RBI, presided over the inaugural session. Shri. Jagdish Capoor, Deputy Governor, RBI, Shri. M.G. Srivastava, ED, RBI and Dr.V.P. Gulati, were the other dignitaries on the dais.

In his welcome address, Dr. V.P. Gulati, Director, IDRBT, outlined the initiatives taken by IDRBT from its inception for technology upgradation in the banking industry. He recalled the historic inauguration of the Indian Financial Network (INFINET) in June 1999, which was a major landmark in enabling technology upgradation in the banking sector.

With the INFINET infrastructure in place, it is now for the Banks to come out with applications to optimally utilise the capacity of this unique, secure, country-wide communication backbone exclusively created for them, he said. Banks could concentrate on using the INFINET for their intra-bank applications and connectivity requirements, which constitute the bulk of their business and transactions. He also solved three myths:

Myth No.1: The INFINET is costlier than some commercial networking options.

Reality: *The INFINET charges are far less than that of any private commercial vendor. And INFINET being a non-profit-oriented venture, charges are closely related to the costs incurred.*

Myth No.2: The INFINET is meant only for inter-bank connectivity and hence banks need to develop their own corporate network separately and link it with INFINET for inter-bank connectivity.

Reality: *Banks need not have two separate networks. They can plan in such a way that they use INFINET to create a corporate network for them and fill in the gaps, with dial-up or leased lines. Since intra-bank applications and transactions form the bulk of any bank's business, the INFINET would effectively serve the purpose of being the backbone for a countrywide corporate network for a bank.*

Myth No.3: The INFINET does not provide adequate security.

Reality: *He assured the bankers that INFINET is the most secure communication network using state-of-the-art technology since at the Network Level:*

- The IP addresses of the remote IDUs are allotted and maintained by the HUB and cannot be changed by the end users.
- In the space segment, the VSATs use a proprietary standard for encryption even in broadcast mode and packets cannot be opened by any VSAT, other than the one specified as the destination VSAT.
- On the Leased Line Network, IPSEC will be used to provide state-of-the-art security.
- PKI will soon be made available on the INFINET to provide security at the application level.

Dr.Gulati expected the Structured Financial Messaging Solution (SFMS) to be in place within six months. He pointed out that the banks can use SFMS for most of their intra-bank applications and

SFMS would be closely integrated with the emerging inter-bank solutions, namely, the Real Time Gross Settlements System (RTGS) and the Centralised Funds Management System (CFMS).

Dr. V.P. Gulati, Director, IDRBT; S.P. Talwar, Deputy Governor, RBI; Shri Jagdish Capoor, Deputy Governor, RBI and Shri M.G. Srivastava, ED, RBI (left to right) at the inaugural session.

Shri. S.P. Talwar, Deputy Governor, RBI, in his address emphasised the importance of this conference, focussing on the technology in banks to improve efficiency in operations, provide better customer service, strengthen MIS and upgrade housekeeping. The urgent need for the Public Sector Banks to effectively compete with the new private sector banks and foreign banks, is looming large, he said, with the business share of the PSBs dipping every year.

Stressing that the infrastructure provided by the INFINET was a major milestone, with 5000 VSATs planned to be deployed in over 126 important cities across the country, he advised that the National Payment Council (NPC) which meets every month, discuss the progress made by PSBs in Technology Upgradation.

Regarding the compliance with the CVC guidelines on computerisation, Shri. Talwar informed that three banks - SBI, Corporation Bank and Oriental Bank of Commerce have achieved the target of 70%. Nine banks are in the range of 60-70% and are planning to reach the stipulated level by March 2001. Fifteen more banks are yet to rise to the occasion and out of these six banks are below the 40% mark.

Shri Talwar advised the bank chiefs to accord top priority to intra-bank applications and connectivity. Banks should draw up a concrete plan for utilisation of the INFINET and to network their branches and offices, he said and asked the DIT, RBI to write to the banks in this regard. Banks can count on help and support from IDRBT and RBI in their endeavour of networking, he said.

As a strategic initiative, the PSBs must set up a Core Working Group on Technology in each bank and this Core Group can have interactions at regular intervals with IDRBT and DIT of RBI. Outlining the role of the Core Group, he said, it would:

- Study the existing I.T infrastructure in the bank and its usage.
- Plan for using the INFINET to the optimum level by implementing intra-bank and inter-bank applications.
- Develop an Enterprise Network for the bank using the INFINET infrastructure supplemented with leased line (intra-city/nearby city), ISDN, Dial-up etc connectivity.
- Carry out a cost benefit analysis on the I.T. investment.

This was followed by two presentations:

a) Enabling Technologies to Build Applications on INFINET, SFMS, MMS by Shri. K.R. Ganapathy, Adviser, IDRBT.

b) RBI Initiatives on Technology Implementation by Shri. S. R. Mittal, Chief General Manager, DIT, RBI.

Both the presentations dealt with the issues in greater detail and answered some of the basic doubts of the participants. Some of the points, which emerged from the discussion, which followed, were:

- Banks to have their own arrangements for intra-city networking. INFINET to provide only inter-city connectivity.
- Bank Gateways will have enough capacity to take care of the bank's requirements. The detailed specifications would be given to banks. The need for multiple gateways for banks would be examined if and when required and the SFMS provides for multiple gateways.
- Bandwidth is not a problem at all. If the banks inform IDRBT of their applications and requirements, enough bandwidth can be provided on demand.
- RBI has set up a group for Internal Inspection and Audit of systems and software applications and the recommendations and procedures would be circulated to the banks as and when the group submits the report.
- The Leased Line Network may be in place within 3-4 months.
- The ceiling of Rs.5.00 lakhs on EFT may go within 6 months.

A generic draft for Perspective I.T. Planning may be given to banks, from IDRBT/RBI so that the banks could use them while drawing up their own plans keeping in view bank-specific issues, constraints etc.

Dr. Gulati also announced that IDRBT has set up five Working Groups for focussed study, as follows:

1. Design and Development of Network Architecture for Financial Applications.
2. Software Architecture for Banks
3. Security Related Technologies.
4. Electronic Presentment and Payments
5. Business Intelligence.

These groups will have professional bankers, I.T experts, RBI representatives, academicians and IDRBT Faculty as members, he said. The inaugural session ended with a Vote of Thanks by Shri.V.Visweswar, Faculty, IDRBT.

The afternoon session was meant for detailed deliberations with DIT Chiefs and their representatives from PSBs on the issues in four major areas of technology implementation and upgradation, as follows:

1. Network Architecture (Corporate) and Design.
2. Mail Messaging Solution.
3. Structured Financial Messaging Solution
4. Intra-Bank and Inter-Bank Applications

The various issues, which came up for discussion during the meeting, are:

- Benefit of IT yet to reach customers. Banks to take a closer look at this aspect.
- Long-term perspective for centralized Vs. decentralized systems. Bank-specific plans to be prepared.
- Preparation of a thorough SRS is essential for successful implementation of any I.T plan, system or application.
- Selection of consultants - need for caution and comprehensive criteria.
- Commonality of problems faced by PSBs with regard to IT.
- Necessity to pool resources and share experiences.
- Necessity to allow multiple networks to connect each other. DoT liberalization awaited.
- Duplication in WAN resources should be avoided.
- Common network design and architecture.
- Need for IDRBT to guide banks in network architecture.
- Workshops to be held for a group of banks to study and suggest ways for network design and to discuss micro-level issues.
- Core groups to be formed from both business and IT personnel.
- Settlement in Internet banking was a Pandora's box.
- Corporate e-mails was the first step in implementing application software on the INFINET.
- Mail messaging with digital certificates was a reality on the INFINET today.
- SFMS is progressing steadily with SRS nearing completion and pilot project already planned.
- Message standards report is already in circulation to all banks. Banks to study the message formats relating to securities transactions etc., and give feedback to speed up the process of implementation.

Deliberations in the afternoon….. DIT Chiefs and their representatives

- Unused INFINET IP Addresses to be surrendered by banks to IDRBT so that they can be centrally administered.
- Now that Linux is getting support from major vendors in the industry, it may be taken seriously as a viable OS alternative for wider acceptance in banks.
- Need to be cautious as far as Internet Banking is concerned.
- Banks have to be clear about what they want to do in terms of applications and requirements before they go in for a networking solution.

With a vote of thanks by Shri Aditya Gaiha, Faculty, IDRBT, the curtains came down on the day-long deliberations. ■

National Seminar on Information Technology Laws and Intellectual Property Rights

A two-day National Seminar on Information Technology Laws and Intellectual Property Rights was held at the Institute on 11th and 12th December, 2000. Organised jointly by IDRBT and Lex Orbis - a firm of attorneys specializing in IT Laws, in association with the Ministry of HRD, Copy Right Division, Govt of India and the World Intellectual Property Organization, the seminar focussed on the interplay between Technology and Laws relating to Intellectual Property Rights.

Shri. J. Satyanarayana at the inaugural session

Shri J. Satyanarayana, Secretary, Ministry of Information Technology, Government of Andhra Pradesh, inaugurated it on behalf of Shri N. Chandrababu Naidu, Hon'ble Chief Minister of Andhra Pradesh, and read out his address. The Chief Minister focussed on the need for a separate set of laws to regulate and govern the cyber economy. "This was essential because the subject matter in the cyber world is intangible and exists in the unseen digital world that defies the normal, time-tested methods of evidence and assurance. Secondly, the traditional methods of jurisprudence are too slow for the Internet World."

Pointing out that India is among the 13 countries that have enacted legislation in the shape of the IT Act 2000, which provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, he said that the Act essentially brings two fundamental changes: it gives legal recognition to the records maintained electronically and to the process of authentication of electronic records by fixing digital signatures.

Delivering the keynote address, Dr. V.P. Gulati, Director, IDRBT, emphasised that in today's knowledge economy, the haves and have-nots and the rich and the not-so-rich are identified by the amount of information they have and the relative ease with which one can gain access to the information they need. Thus the harmonisation of Intellectual property has to be accorded top priority.

"India has many things of value that need to be protected from exploitation. Therefore, information security is a necessity for India to continue to enjoy its rich cultural heritage," Dr. Gulati stressed.

Several speakers of international repute and eminence participated in the seminar. Soh Kar Liang, an advocate & solicitor of the Supreme Court of Singapore spoke on E-Commerce Laws in Singapore; and on Domain Name Protection, Conflicts and Consensus; Robert Miller, Principal, Spruson & Fergusson, on Computer Software Patentability; J. Satyanarayana, Secretary, MIT, Govt of AP, on E- Governance; S.R. Mittal, CGM, IT, RBI, on Payment & Settlement Systems in the Digital Environment - Legal Concerns, and on Legal Concerns Associated with Payment and Settlement systems in Digital Environment; K. N Gupta, Controller of Certifying Authorities, IT, on Cryptography for Electronic Commerce in India, Gladys Mirandah, Co-founder and Managing Director of ecgm, on Domain Names - Singapore, Patrick Mirandah, founder of Patrick Mirandah Sdn Bhd, on Domain Names - Malaysia, and Shri V. Visweswar, Faculty, IDRBT, and the Programme Coordinator on Domain Name Registration - India.

Chief Minister Shri N. Chandrababu Naidu with the foreign delegates

A large number of Executives/Decision Makers from the IT Industry, Banks, Financial Institutions and Government Agencies participated in the seminar and it was a huge success. ■

Executive Development Programmes

Payment Systems and Information Security Strategies

This one-week programme, held at the Institute, from November 20-25, 2000, provided exposure to the participants on the need for a Strategic Security Architecture, Risks associated with Payment Systems and their management, Security Technologies, and Cryptography Systems.

Executives from various banks including two foreign delegates from the Central Bank of Sri Lanka participated in the programme.

Apart from the Faculty of the Institute, experts from the Reserve Bank of India, and Guest Faculty from the Industry delivered lectures in the programme. The programme was highly appreciated.

Dr. Ashutosh Saxena coordinated the programme.

Enterprise-wide Networking

Two programmes on Enterprise-wide Networking were conducted from Nov 13-18 and from Dec 18-23, 2000.

While there were 26 participants in the first programme, the second programme had 31 participants. The participants were Managers and Executives from CPPD/DIT of both Public and Private Sector banks, who are responsible for Network Management.

Participants of the programme on Enterprise wide Networking for Oriental Bank of Commerce

A wide range of topics including Networking Concepts, Design and Implementation of LAN, IP Addressing System, VSAT Technology, Mail Messaging System, Intrusion Detection system, and Network Directory Services were discussed.

These programmes were coordinated by Shri N. Rajendran and Shri Varghese Jacob.

An exclusive programme on Enterprise-wide Networking was also conducted for Oriental Bank of Commerce from January 15 - 20, 2001. Twenty-five participants from various branches of the Bank participated in the programme. The Executive Director of OBC, Shri V.K. Chopra participated in the valedictory function of the programme.

This programme was coordinated by Shri. Varghese Jacob.

E-Commerce and Payment Technologies

This programme, held at the Institute from December 04-09, 2000, aimed at familiarizing the participants with Business Models and Emerging Trends in E-Commerce, Payment Protocols over Internet, Internet and Security Technologies, Internet Banking, Legal and other Issues.

The participants of the programme were Managers and Executives from CPPD/DIT and Business Planning Departments who are directly responsible for design, development, and Implementation of Software Systems and Policy formulation for E-Commerce.

Participants from Union Bank of India, Oriental Bank of Commerce, Bank of Baroda, State Bank of Indore, Reserve Bank of India, and United Bank of India participated.

Shri A.R. Dani coordinated the programme. ■

Other Events

Workshop on SRS for SFMS

A 2-day workshop for review and finalisation of System Requirement Specifications (SRS) for Structured Financial Messaging Solution was conducted on January 03-04, 2001. Representatives from participating banks, IDRBT, and the SFMS development team from Tata Consultancy Services attended the workshop.

Features of SFMS, requirements of banks from SFMS, APIs required at the bank branch front end, security features, and usage of smart cards were discussed.

The participants also deliberated on ISN & OSN sequencing and numbering of messages originating from bank branches, rejection of messages based on various criteria, message versions, action to be taken in case of failure at HUB & Gateway, user profile & authorization, training messages, broadcasting of messages from HUB and Gateway, multicasting of messages and related policy decisions.

The changes necessary in PKI-based (Public Key Infrastructure) security in accordance with the new IT Laws were communicated to the representatives.

The hardware and software environments for the pilot project were discussed and banks were advised regarding the requirements of the bank gateways.

Forthcoming Programmes

International Seminar on Payment & Settlement Systems - Challenges for Emerging Economies (March 14 - 17, 2001)

The Reserve Bank of India and IDRBT in association with Bank for International Settlements will conduct an International Seminar on Payment & Settlement Systems - Challenges for Emerging Economies, from March 14 -17, 2001.

The seminar aims to explain the structure and functioning of Payment and Settlement Systems in the modern market economy. The focus will be on the policy issues relating to Payment Systems, in particular those seen from the National Payment Council's Perspective. The intention is to familiarise Payment System Experts with the developments and related policy issues on the global front.

Participants will, therefore, obtain a good view of the role of Central Banks, Commercial Banks and Financial Institutions in managing change in Payment Systems and also of the key objectives of Payment Systems reform.

While the primary attention will be on the economic, financial and legal aspects of the payment systems, i.e., how payment and settlement systems form part of an efficient, stable, and competitive banking and financial Industry, attention would also be paid on the technology and security aspects of building Payment and Settlement Systems.

The topics to be deliberated upon include Funds Transfer System, Delivery Vs Payment, Foreign Exchange Clearance, legal and technology aspects.

The seminar will include a number of presentations and group discussions by the officials from Bank for International Settlements, various G-10 member central Banks, and central Banks of Asia and Africa.

Central Banks of the SAARC countries, Singapore, Thailand, Indonesia, Philippines, and other developing countries are expected to participate in the seminar.

For further information, please contact the programme coordinator:
Shri V.Visweswar.
e-mail: viswar@idrbt.ac.in

Top Management Seminars on Banking Technology
Bank of Baroda, February 13-14, 2001
Punjab National Bank, February 15-16, 2001
Oriental Bank of Commerce, February, 22-23, 2001

These seminars on Banking Technology for the top managements, aim at disseminating knowledge on Emerging Trends in Banking Technology.

The issues to be discussed include Banking Technology and Change Management, Financial Network Architecture, Corporate Network for Bank and Banking Applications, Corporate e-mail, Mail Messaging System, Electronic Commerce and Internet Banking, Network Security, Cryptography, Certification and PKI, IT Project Management etc

Banking Technology & Internet Based Training (March 19-28, 2001)

This 10-day programme, targeted at the Faculty members of the Staff Training Colleges and Executives from HRD & Training Divisions of Banks and Financial Institutions, aims at enabling the participants to understand the emerging trends in Banking Technology, Payment Systems, E-commerce, and Internet Banking.

The major topics, which will be addressed, include Financial Network and Banking Applications, Decision Support Systems, Usage of Electronic Spread Sheets and Databases, Intranets and Internet, Web Design concepts, Web based learning standards and development tools, Multimedia and Computer simulation and issues involved in implementing web based training.

Participants from within the country and abroad are expected to attend the programme.

For further information, please contact the programme coordinators:

Dr. V.N. Sastry, e-mail: vnsastry@idrbt.ac.in
Shri. M.V. Sivakumaran, sivakumaran@idrbt.ac.in

Data Warehousing & Business Intelligence for Banks and Financial Institutions

(April 16-21, 2001)

This programme, scheduled to be held at the Institute from April 16-21, aims at disseminating knowledge on Data Warehouse relevant to the Banking and Financial Sector.

The programme will cover the Concepts of Data Warehousing, Strategy Planning Process, Mapping Organisational Needs, implementation Details, Online Analytical processing, Data Marts, Data Mining and Banking Applications. Discussions will focus on the Comparative strategies of Data Warehousing of various banks and the steps initiated to start and manage the Data Warehouse Project.

Executives and Managers responsible for DW Design, development and Implementation and Faculty from Staff Training Colleges can attend the programme.

For further information, please contact the programme coordinator:

Dr. P. Radhakrishna, e-mail: krishna@idrbt.ac.in

ON THE ANVIL

M.Tech Programme in Banking Technology and Information Security

IDRBT in association with University of Hyderabad is planning to offer an M.Tech Programme in Banking Technology and Information Security from the next academic year, i.e., June 2001.

It is a three-semester (1 ½ years) full time programme, which seeks to merge the new and emerging trends in Information Technology with the domain expertise in the ever-changing field of banking and financial services. The programme, as it is envisaged, will be a powerful launching pad for a highly rewarding professional career in Banking Technology and Information Security. Focusing on both technological and business perspectives, this programme addresses challenges and solutions associated with Banking and Finance. It will have courses on the core areas of Banking Technology, Computers and Information Security.

The programme is open to both direct and sponsored candidates. Admissions will be strictly on the basis of merit: scores in the written test and performance at the interview.

Web Based Post Graduate Programme on Banking Technology Management.

IDRBT is planning to start a Web based Post Graduate Programme in Banking Technology Management (PGP-BTM) shortly. The objective of this programme is to impart state-of-the-art knowledge of technology and its management relevant for modern Banking and Financial Services to meet the emerging challenges in this Information Era. This programme will be useful for graduates already working in a Bank.

It will be a web based learning programme of two years, in a virtual classroom scenario through the Internet. The Institute will take the assistance of Faculty from the Staff Training Colleges of Banks to act as mentors and regional/bank level coordinators for better interaction between the learners and the teachers.

It is also proposed to have a one-week contact programme for the participants every year. There will be a live project apart from a number of real-life case studies to enable the students apply their knowledge to provide solutions.The programme aims at making the best use of the technology available to make this online learning experience cost-effective, empowering and rewarding for the students.

Watch out for more details on our website: http://www.idrbt.com / and the next issue of this newsletter.

INFINET News

The INFINET now has 504 VSATs commissioned across the country. The inroutes of the INFINET are being further expanded from the present 16 to 32. The proposal is under final stages of approval.

More than 35 foreign banks, private sector banks, and co-operative banks have evinced keen interest in joining the network as CUG members.

A specially formed sub-group of the INFINET Users' Group had a meeting at IDRBT to deliberate and finalise the modalities and pricing for Annual Maintenance Contract for the VSATs, which will be applicable from the date of completion of warranty of the VSATs. The recommendations of the group are being forwarded to the Chairman, INFINET Users' Group.

Digital Certificates for secure e-mail will be shortly available on the INFINET. The final testing for implementation of the system is currently on.

All IPs used by the CUG members for the INFINET have to be necessarily registered with IDRBT. All traffic, other than the valid 10.X.X.X traffic, has been blocked on the INFINET since 1st February 2001. All unregistered IP Traffic will also be blocked on the INFINET from 15th February, 2001.

Structured Financial Messaging Solution

System Requirement Specifications (SRS) for Structured Financial Messaging Solution (SFMS) is now ready. Tenders for hardware and software at HUB as well as at bank gateways for SFMS Pilot Project were floated. The technical and commercial bids have been received. The Technical Committee met on January 22, 2001 to discuss technical bids from vendors.

Mail Messaging System

IDRBT has been advising all the banks to use the Mail Messaging System (MMS) of the INFINET. To bring uniformity among all the bankers, all users can implement a corporate e-mail directory, which is generic in nature, easily. All the banks should have their domain name as <bankname.co.in>. It is also suggested that every bank evolve a policy of providing one office e-mail and one demi-official address. For simplicity, office e-mail will have the following categories:

designation@bankname.co.in

Examples:

CMD : cmd@bankname.co.in
ED : ed@bankname.co.in
GM (Operations): gmop@bankname.co.in
GM (Credit): gmcre@bankname.co.in
GM : (Planning): gmpl@bankname.co.in

In respect of Zonal Offices, Regional Offices and senior dignitaries located at places other than Central Office, they should adopt:
designation-location@bankname.co.in.

Examples:

Zonal Manager in Delhi: zmdel@bankname.co.in
RM in Mumbai: rmmum@bankname.co.in
DM in Hyderabad: dmhyd@bankname.co.in
In respect of all the branches, they would adopt:
Branch-Manager-Location-Code@bankname.co.in.

For example: Ahmedabad branch (code number 0773), Ahmednagar branch (code number 0024) and Bangalore branch (code number 0162) will adopt the following e-mail addresses:

Ahmedabad Branch: bmahm0773@bankname.co.in
Ahmednagar Branch:bmahe0024@bankname.co.in
Bangalore Branch:bmban0162@bankname.co.in

For personal e-mail, if alloted, the e-mail address will be name@bankname.co.in. ■

Working Paper No. 5

The Institute has published its fifth Working Paper. It is on **"Technology for Forex Risk Management - Delta Normal Method for Risk Analysis"** by ***Shri Aditya Gaiha*** and ***Dr.Supriya Kumar De.***

With the opening up of financial markets and globalisation of risks, the area of risk analysis and the various methodologies there of have assumed foremost importance for treasury managers the world over, including those in our country. Technology is one of the important tools used by modern finance managers to manage risks. This paper discusses one of the methods, considered suitable for Indian conditions for dealing with forex risks. ■

Awareness Series

Intrusion Detection Systems

Dr. Supriya Kumar De, Faculty, IDRBT

It's now a world of international networks and electronic commerce, where we can do almost every kind of shopping from the cool precincts of our drawing rooms. Just get connected to the Net and one can reach out to the world. Internet has changed our life. But at the same time, Internet has also brought along many problems, the most important being computer security. Almost every computer on the Internet is a potential target of attack.

Organizations began connecting their mission-critical computers to the Internet for information sharing, business through Internet, and entertainment etc. However, these mission-critical computers were exposed and their security was under threat. As the scale of potential damage due to the attacks by intruders spiraled, the security of the network assumed primary importance. A number of technologies such as Firewalls, encryption technology, authentication devices, vulnerability checking tools, and other products can be employed for defending the network.

Even though the system is equipped with these stringent authentication procedures and firewalls, it is still susceptible to hackers, who can succeed with the help of some social engineering tricks like, acquiring password by impersonating as system administrator or by stealing the password file. Even systems not connected to public networks are vulnerable to attacks from disgruntled employees or other insiders who misuse their privileges. Therefore, it is sensible to establish a second line of defence in the form of an Intrusion Detection System.

1. Intrusions

An intruder is somebody ("hacker" or "cracker") attempting to break into or misuse the system. The word "misuse" is broad, and can reflect something as severe as stealing confidential data to something as trivial as misusing the e-mail system for Spam (junk e-mail). In other words, an intrusion attempt or a threat is defined as the potential possibility of a deliberate unauthorized attempt to access or manipulate information or render a system unreliable or ineffectual. Intruders can be classified into two categories - those who come from outside the network and legitimate users on the internal network. Outside intruders may come through the Internet, dial-up lines, physical break-ins, or some partners like customers, vendors etc., that is linked to the corporate network. Inside intruders misuse their privileges or impersonate higher privileged users. A frequently quoted statistic is that insiders commit 80% of the security breaches.

Intrusions fall into three categories:

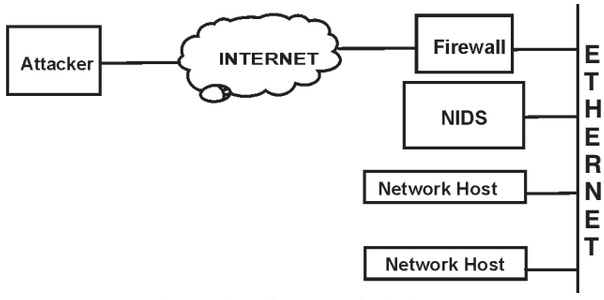
- Physical Intrusion: If an intruder has physical access to a machine.
- System Intrusion: The intruder has a low-privilege user account on the system.
- Remote Intrusion: An intruder attempts to penetrate a system remotely across the network.

Most people use their names, spouse or children's name, car number or no password as their password. This provides a list of nearly 30 possibilities for the intruders to get into the system. A number of protocols (Telnet, FTP etc.) use clear-text passwords. For accessing such passwords, intruders with a protocol analyzer can watch the wire between the client and the server. However, most protocols use some sort of encrypted passwords. In such cases, intruders try to decrypt it by Dictionary attack or Brute Force attack. In Dictionary attack, the intruders will use a program that will try every possible word in a database, whereas in Brute Force attack, the intruders may try all possible combinations of characters.

Bug free software is still a dream. System administrators, programmers, and developers can never track down and eliminate all possible holes. In order to get access to the system, the intruder will have to find only one hole. Software bugs are exploited in the server daemons, the client applications, the network stack and the different operating systems. Even if a software implementation is cent-per-cent in accordance with the design, there may still be bugs in the design itself. For example, in TCP/IP there are a number of design flaws. Hackers

forge and change IP data with impunity. Such TCP/IP flaws give birth to a lot of attacks such as IP spoofing, SYN floods etc., which can be exploited by the intruders.

To begin with, intruders try to find out as much as possible about your network, along with the domain name of the network (such as idrbt.com) by appearing as a normal user or impersonating as system administrator on the phone. At this stage, one really cannot detect them, even if the intruders use more invasive techniques to scan for information. They still do not do anything harmful. The intruders will browse other public information, such as your public web sites and anonymous FTP sites. He might do a TCP/UDP scan on target machines in order to see what services are available on it or to find free ports to enter the system. At this point, the intruders have done 'normal' activity on the network and have not done anything that can be classified as an intrusion.



NIDS in a Simple Network Architecture

Later on, intruders start exploiting possible holes in the target machines. The intruders might attempt to exploit well-known buffer-overrun holes by sending large amounts of data. The intruders' main goal is to hide evidence of the attacks (doctoring the audit trail and log files) and make sure they can get back whenever they want. They may install 'toolkits' that give them access, replace existing services with their own Trojan horses that have backdoor passwords, or create their own user accounts. The intruders will then use the system as a stepping-stone to other systems, since most networks have fewer defenses from inside attacks. The intruders take advantage of their status to steal confidential data, misuse system resources (i.e. stage attacks at other sites from your site), or deface web pages. The intruders may use Denial-of-Service (DoS) attacks, to crash a service (or the machine), overload network links, overloaded the CPU, or fill up the disk. The intruder is not trying to gain information, but to simply act as a vandal to prevent you from using your own machines

2. Intrusion Detection

Intrusion Detection Systems can be classified according to their data sources and their manner of intrusion. Some Intrusion Detection Systems (IDS) are based on audit logs provided by the operating system i.e. detecting attacks by watching for suspicious patterns of activity on a single computer system. This type of IDS called Host-based IDS is good at discerning attacks that are initiated by local users, which involve misuse of the capabilities of one system. The Host-based IDS (HIDS) can interpret only high level logging information and they cannot detect low-level network events such as Denial of Service attacks. The network-based approach can be effectively used to detect these low-level Denial of Service attacks.

Basically, IDS can be classified into two broad groups: Anomaly Detection and Misuse Detection. Anomaly Detection Systems analyse system information and use statistical techniques to search for intrusions by comparing the new behavioural pattern with the normal patterns. Misuse detection tries to detect intrusion by searching for behaviour that matches a known pattern of intrusion activity.

2.1 Host-based Intrusion Detection Systems:

Host-based Intrusion Detection Systems (HIDS) are based on audit logs provided by the operating system. The threats that are addressed by audit trial analysis can be:

- External penetrators: Unauthorized users of the computer
- Internal penetrators: Authorized user of the computer but not authorized for the data, program, or resource accessed of, including
  - ★ Masqueraders: Those who operate under another user's id and password
  - ★ Clandestine users: Those who evade auditing and access controls.
- Misfeasors: Authorized users who misuse their privileges (those found guilty of misfeasance).

External penetrators can be detected by auditing failed login attempts, whereas internal penetrators can be detected by observing failed access attempts

to files, programs and other resources. Masqueraders can be detected by observing deviations from established patterns of use for individual users. Clandestine attacks can be detected by auditing all use of functions and the system service.

The main disadvantage of HIDS is the weak security associated with the system logs and decreased performance of system logs and audit trails because of large size of audit and log files. The main advantage of HIDS is the level of granularity of the collected information.

2.2 Network based Intrusion Detection System

Network based Intrusion Detection Systems (NIDS) are based on interpretation of raw network traffic. They attempt to detect attacks by watching for patterns of suspicious activity in this traffic. NIDS are good at discerning attacks that involve low-level manipulation of the network, and can easily correlate attacks against multiple machines on a network. With most computers now attached to networks, it seems natural that we should have network-based IDS approach.

NIDS provides many advantages over Host based IDS. NIDS watches traffic on the wire and is not effected by changes of the server platform.

1. A single NIDS deployed at the access points of the network can watch all the systems on the network.
2. NIDS monitors a wide array of attacks that range from protocol stacks to environment specific attacks.

The main disadvantage of NIDS is that it has a fail open architecture. If an intruder can disable a NIDS, all host on the local area network (LAN) are then left without an IDS. The intruder will do it by overloading the network traffic or crashing the system by Denial of Service attacks. NIDS may create some ``false positives" (perceived threats that appear to the NIDS to be real, but are just normal data transactions) and ``false negatives" (there is an attack, but NIDS treats as the normal activity).

The Network based Intrusion Detection System (NIDS) developed at IDRBT detects the low-level network attacks called Denial of Service attacks. This NIDS gets copies of its network traffic and having its network interface card bring in a copy of every packet it sees. In this process, NIDS does not affect the performance of hosts on the network. It examines these packets, and attempts to determine whether they represent an intrusion attempt. It does this by seeing if the contents of the packet contain a string of characters that matches a specified pattern.

Both NIDS and HIDS have their advantages and disadvantages. Neither of them working alone can detect all intrusion attempts on their own. The future is converging towards designing a model with a distributed approach called Distributed IDS (DIDS). These type of models be designed to automate the collection and analysis of the data from all the hosts as well as Local Area Network (LAN).

[1] J. P. Anderson, Computer Security Threat Monitoring and Surveillance, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980. ■

My Days at IDRBT

By Shri K. R. Ganapathy
Adviser, IDRBT

On the eve of my leaving IDRBT, which is now fully functional and has all the infrastructure required for research and development, and the faculty and staff busy with their research and other assignments, I feel very proud that Reserve Bank of India provided me an opportunity to be associated with this august Institution right from its inception.

My memory flies back to my first day in IDRBT - September 25, 1996, when I started working in the Institute with the Founder Director, Shri W. S. Saraf, Shri M. S. Aradhey, Shri A. S. Kulkarni and subsequently with Shri A. D. Hariharan and others. Those were the days when there was hardly any greenery in the Institute. Neither did the Institute have any infrastructure, except the buildings.

In the first one year, the Institute mainly focused on the setting up of VSAT based satellite communication infrastructure. It was a very

challenging task. We encountered a large number of problems while selecting a suitable vendor. Though the decision regarding the wide area network infrastructure and campus wide networking was taken during the same period, the real implementation could be started only in the last quarter of 1997.

We built a conference room with all modern amenities during the first year and the Institute too had just started looking green. That was when Shri W. S. Saraf retired and Dr. V. P. Gulati took over as the Director.

When I look back, in the last 2½ years, the Institute has made fantastic progress not only in terms of building up the technology infrastructure but also in terms of initiating a number of research and development activities. It is heartening to see that we have an infrastructure that is comparable with the best in the world.

It is not that we did not have problems in the last 2½ years. In spite of it, the Institute took up the challenge of building a modern infrastructure and we came out with flying colours.

The accident, which occurred, during the installation of 11-meter antenna, was a setback and it did affect our schedule but we took it in the right spirit and sorted out the problems. The project was implemented successfully, of course with the support from RBI, Governing Council, the entire banking industry, faculty and staff of IDRBT and the vendors, especially HECL and CMC.

It gives me a sense of pride when the RBI and its top executives, top executives of banks, the participants from banks, guest faculty and other visitors appreciate the Institute's work and its facilities. I have no doubt that under the able leadership provided by Dr. Gulati and the dedicated faculty and staff of the Institute, the Institute is well equipped to achieve the objectives for which the Institute has been set up.

It is with mixed feelings that I am bidding goodbye to the Institute after having been here for 4 years and 4 months - sad that I have to leave the organization I was associated with right from the beginning and happy that I am going back to my parent organization - RBI, where I would continue to work in the area of Information Technology.

I wish the Director, faculty and the staff of the Institute the very best in their endeavour to make IDRBT a centre of excellence in banking technology related areas.

Shri K.R Ganapathy, Adviser with IDRBT since its inception returned to his parent organisation, Reserve Bank of India, recently. He has taken charge as the Head of the Department of Information Technology, Central Office, Mumbai. IDRBT places on record the valuable contribution of Shri K.R. Ganapathy to the Institute. IDRBT wishes him success in all his endeavours.

IN BRIEF

Join IDRBT

Professional Bankers with adequate exposure in I.T are welcome to join IDRBT as Faculty on Deputation, Project Associates or Research Fellows.

* * *

Workshops

Two-day Workshops for Core Groups from Banks are scheduled to be held in six batches in April, 2001.

* * *

Invitation

We invite contributions from our readers on specific areas of Banking Technology for publication. Case studies are also welcome.

For details, please visit our website.

- Editor

Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad - 500 057, India.
EPABX : 3534981-84 (4 lines), Fax : (040)-3535157, 3536361
e-mail : publisher@idrbt.ac.in , Website:http://www.idrbt.com