IDRBT

The Think - tank for Banking Technology

FAST FORWARD

A Quarterly Newsletter

from

IDRBT

Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Hyderabad - 500 057, INDIA.

Vol : 3 June 2000 No: 3& 4

Executive Development Programmes

Workshop for Regional Directors and Chief General Managers - in -Charge of Reserve Bank of India.

This two-day high level Workshop was organised by IDRBT at the Institute Campus in Hyderabad (April 21-22, 2000). The purpose of the workshop was to familiarise the participants with the INFINET infrastructure, the emerging trends in I.T and Banking Technology and to discuss the I.T. Strategy for RBI for the next five years. The workshop was attended by the Regional Directors of Reserve Bank of India, from all over the country and Chief General Managers-in-Charge of the Departments in Central Office, Mumbai. In all, there were 30 participants.

Shri. S.P. Talwar, Deputy Governor, (third from left) flanked by the other dignitaries during the inaugural session of the workshop.

Dr.V.P. Gulati, Director, IDRBT, delivered the Welcome Address. The workshop was inaugurated by Shri.S.P. Talwar, Deputy Governor of the Reserve Bank of India. Dr.A. Vasudevan and Shri.M.G. Srivastava, Executive Directors of RBI made presentations and were present throughout the workshop to guide the deliberations. Issues like standardisation and seamless integration of the systems and applications that are already in use and the possibilities and priorities of technology upgradation across the Bank were also discussed in the workshop. Experts provided inputs on emerging trends in Banking Technology, Financial Networking and Internet Banking to the participants of the workshop.

Workshop for CPPD/IT Dept. Chiefs on Security Policy and INFINET Related Issues

This 3-Day Workshop, organised at IDRBT Campus, from 27-29 April 2000, was meant for Computer Policy and Planning Division Chiefs of Public Sector Banks. The thrust of the workshop was on the nitty-gritty involved in evolving and implementing a Sound Security Policy for the

Prof. Longley addressing the participants on Security Policy. Also seen in the picture are(to his left): Shri.K.R.Ganapathy, Adviser, IDRBT, Dr.V.P. Gulati, Director, IDRBT and Dr.A.Saxena, Programme Coordinator.

computerised environment within the Bank as well as for inter-bank connectivity and applications. In his opening remarks Dr.V.P. Gulati, Director, IDRBT, stressed the need for security on INFINET and mentioned the various initiatives being taken at IDRBT in this area. He also mentioned that certification services would be made available, shortly, on the messaging backbone(MS Exchange) on INFINET. Prof. Longley from Queensland University of Technology, Australia, inaugurated the workshop and also delivered a lecture, later on, on the architecture of a Security Policy and the key considerations involved in evolving a policy which can be implemented effectively.

The steps required to be taken for optimum utilisation of the INFINET infrastructure were also addressed during this workshop. Live demonstrations were organised during the workshop on Intrusion Detection Systems and Digital Certificates for Secure and Certified Email.

Special Programme for Bank of Maharashtra

Bank of Maharashtra had requested IDRBT to conduct a Special Executive Development Programme on Emerging Trends in Technology for their top executives. We have conducted this one-week programme for two batches in January-February 2000, covering around 30 top executives of the Bank, most of them GMs and DGMs. The topics covered included a wide range: MS Excel, Email, Intranets and Internet, Risk Management, Security Technologies, Intrusion Detection Systems, INFINET, Smart Cards, Payment Systems and other emerging technologies. The programme was very well received and appreciated. One more programme is scheduled to be held in August 2000.

Special Programme for Canara Bank

At the request of Canara Bank, a two-day Special Executive Development Programme was conducted on "INFINET and Emerging Trends in Technology" for their General Managers (June 30 and July 1, 2000). There were 18 participants. The programme was inaugurated by Shri. R.J. Kamath, Chairman and Managing Director of Canara Bank. The topics covered included: INFINET, Intranets, Intra-bank and Inter-Bank Applications, Corporate Email and Messaging, Security Technologies, Data Mining and Data Warehousing. The programme was well received.

Training Programmes on Messaging Systems

We have conducted six training programmes (as against four scheduled originally) on MS Exchange between January and April 2000, for the benefit of those Banks which have chosen MS Exchange as their messaging backbone. A total of 120 participants were trained in these programmes. The participants were from Allahabad Bank, Bank of Baroda, Oriental Bank of Commerce and Reserve Bank of India. The programme had technical sessions and provided hands-on training for the participants in configuration, maintenance and trouble shooting of the backbone.

Workshop on Security on Messaging Systems

A workshop was conducted from April 6-8, 2000, to enable the Technical Staff of the Banks to configure clients/servers/certification servers etc., of the different messaging systems. During the workshop, demonstration of the three messaging backnones, viz., MS Exchange, Novell Groupwise and Lotus Notes was arranged with the help of the vendors. The workshop laid more emphasis on security on the messaging backbone and for this purpose demonstrations also covered the key aspects of digital certificates, certificate servers etc. There were 35 participants in this workshop, drawn from the PSBs and RBI.

The participants (GMs) of the Canara Bank Programme, with Shri.R.J. Kamath, their CMD, Director, IDRBT and Faculty.

Other Seminars and Events at IDRBT

Price Waterhouse Coopers, Hyderabad, made a presentation on "Public Key Infrastructure and other Security Related Issues" on 17th January 2000.

Microsoft Corporation made a presentation on "Windows 2000 and Security Features" on 10th February 2000.

Tata Consultancy Services made a presentation on "Asset Liability Management Software Solutions" on 23rd February 2000.

Forthcoming Programmes

Programme on Novell Groupwise (July 17-22, 2000)

This one-week programme is being organised for the benefit of those banks which have selected Novell Groupwise as their messaging backbone. The participants would be System Administrators, Technical Support Staff and Trainers from Banks and Financial Institutions.

For further information please contact the Programme Coordinator: Dr.V.N. Sastry
Faculty, IDRBT
(Email:vnsastry@idrbt.ernet.in)

Special Programme for CBI Officials on Information Security and Cyber Crimes (July 24-28, 2000)

A 5-Day Executive Development Programme is being organised, exclusively for CBI Officials, on Information Security and Cyber Crimes in the Computerised Environment. This programme will focus on the skills and techniques required to handle cyber crimes. The participants will have an insight into the various aspects like security breaches in computerised environment, detection of cyber crimes, collection of evidence, legalities involved in producing and proving evidence in electronic form, reorientation needed for handling cyber crimes etc. The programme will focus exclusively on tackling cyber crimes in the key sectors of Banking and Finance. Participants will be: DIGs, SPs and DSPs of the Central Bureau of Investigation from all over the country.

For further information please contact the Programme Coordinator: Dr. P. Radhakrishna
Faculty, IDRBT
(Email:krishna@idrbt.ernet.in)

Web Based Learning (August 7-12, 2000)

This one-week Executive Development Programme seeks to prepare the Bankers for the emerging system of Web Based Learning and Training. The programme seeks to familiarise the participants with the issues involved in and the tools required for Web Based Learning Systems.

The Programme is meant for Bankers: Faculty Members from the Training System and Executives from HRD.

Last Date for Registration: 17th July 2000.

For further information please contact the Programme Coordinator: Shri.M.V. Sivakumaran
Faculty, IDRBT.
(Email:sivakumaran@idrbt.ernet.in)

Special Programme for Bank of Maharashtra

One more Special Executive Development Programme is scheduled to be held for the top management of Bank of Maharashtra from August 21-26, 2000.(Programme details available on Page 2 of this Issue.)

INFINET News

The INFINET network, which was inaugurated on 19th June 1999, has been in operation for over a year now with 439 VSATs already commissioned across the country. The CUG member banks have started using the network for email and various other intra-bank applications.

Full Transponder Allocated on INSAT 3B

A full transponder (No. 8) has been allocated for INFINET on the recently launched INSAT 3B. Since INSAT 3B is not co-located with INSAT 2B reorientation of the antennas both at the hub and the remote sites is mandatory. A full-fledged schedule for the same is being worked out in order to cause minimum downtime of the network. This will involve a massive coordination among the Institute, CUG members and M/s.HECL. With this shift from one eighth of a transponder to a full transponder there will be better bandwidth availability on the VSAT based network itself.

E-mail backbone on INFINET

In order to encourage usage of the network amongst the CUG members an e-mail backbone with 9 e-mail servers, located at IDRBT were set up and became operational in mid January, 2000. Default e-mail ids were created for all VSAT locations and the installation details for thin clients as well as remote servers were circulated to all CUG members. A large number of training programmes were also held at the Institute in order to help the remote VSAT users to use the mail facility. The usage of this facility has picked up considerably in the recent past.

Email Interface with Internet

Configuration work has been completed at the Hub for providing an Email gateway to the Internet for Banks on the INFINET. The detailed guidelines on the set up and configuration to be done at the user-end have already been circulated to the CUG members.

Corporate Internet E-mail for RBI

Inter-connectivity between Internet and INFINET for the limited purpose of internet mail for the RBI was made operational from 20th April, 2000. Under this system all internet mails sent via the internet to any user in RBI, i.e., user@rbi.org.in will be routed through an internet gateway, located at IDRBT, to the INFINET messaging system and from there to the user and vice versa. This is a major step towards the final goal of integrating the INFINET with the internet for various purposes including Internet Banking. The security provided currently will be strengthened before other internet services are made available through INFINET.

Leased Line Network

A leased line network connecting 21 cities with a mixture of 2Mbps and 64Kbps leased line links which will be seamlessly integrated with the VSAT based INFINET is being set up and shall be completed within six months. This will provide better bandwidth availability for the users of INFINET.

Network Integration Issues

It is advisable for all CUG members to strictly adhere to the IP addressing scheme as formulated by the Institute. The subnet mask 255.255.255.224 is to be strictly adhered to. All LANs at remote locations should access the INFINET WAN via a proxy server acting as a NAT or a router acting as a NAT only. The routers connected to the VSAT WAN should work with static routing RIP version 1 only, for the time being.

Website for INFINET

A separate website for INFINET is being launched at **http://www.infinet.org.in** shortly. The website will provide up-to-date information required for the CUG members. This website will also act as a forum for the banking community to share their views and experiences on intra-bank and inter-bank applications and other ways of using the INFINET infrastructure fully and efficiently. The website will also allow members to have a look at their account details like traffic flow and utilisation patterns.

Update on Research Projects

Certificate Server for E-Commerce

A Software Project is on to develop a Certificate Server for use by Certificate Authority.The Certificate Server will be responsible for the entire Certificate Life cycle Management right from the processing of certificate request to publishing of certificate revocation lists.

Sequence of Operations

- Client connects to CA's Web site
- Exchanges series of messages between Client and CA which involves request and response on
  - Initiation and
  - Registration
- CA stores & validates the data (on/offline)
- CA sends possible time of certificate delivery
- Collection of certificate by client
- Use of certificate by client

The certificate server is developed using JAVA and the entire development is based on Public Key Cryptography System

We have adopted X509.V3 standards for the certification process. We are adopting Lightweight Directory Access Protocol (LDAP) to maintain user details and certificates. We are also in the process of creating Certificate Revocation Lists (CRL).

We are using Digital Signatures on a pilot basis in the Institute for email messages using Outlook2000.

Intrusion Detection Systems

The growing connectivity on the internet brings with it enormous opportunities for attackers to illegally access computers via networks. Hence it is very important that the security mechanisms of a system are designed so as to detect such attacks on the networks. The task of detecting such attacks is called Network Intrusion Detection. In order to understand the collection and use of evidence by intrusion detection systems, it is first important to realize that threats to networked computer system come in a number of forms. For this purpose, we divide the attacks into two classes: Outsider attacks and Insider attacks.

Outsider Attacks : Outsider attacks come from outside your network, and they may attack your external presence like your web server or even your gateway to the outside world or they may even come to your LAN server whenever it gets directly connected to the external world. Outside intruders may come from the internet, dial-up lines, physical break-ins, or from a partner network (vendors, customers, resellers, etc.) that is linked to your corporate network.

Insider Attacks: In insider attacks intruders are legitimate users of your internal network. Their attacks receive less attention. These attacks can be more pernicious and insidious than outsider attacks due to the information and system privileges the legitimate users have.

A frequently quoted statistic is that 80% of the security breaches are committed by insiders.

In computer security terms intrusion detection generally falls into two categories: Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS). NIDS passively examine raw network traffic at a single point on a network. By analysing the packets seen on the network, NIDS try to match "signatures" of intrusive behaviour.

The HIDS on the other hand sit on each Host and use system audit trail data and sometimes other interactively determined system information for detecting intrusions.

Pattern Discovery and Data mining of Loan Data

This is a new project taken up by the Institute in the area of Data Mining. Data Mining is the most suitable approach for banks, having a large amount of data on customers, to get insights into customer preferences, acceptance and usage patterns of different products and services offered etc. It can be defined as the process of extracting hidden and interesting, implicit information (or knowledge) from large databases and then using the knowledge to make crucial business decisions.

The objective of this project is to identify the interesting patterns related to customer profile and asset type in the loan data of a bank using data mining techniques. Profiles of around 300 customers were taken from a bank with details pertaining to occupation, residential address, gross and net income, sanctioned loan amount, outstanding amount and overdues. The data is mined using association rule and classification techniques. For the present study a tool has been developed in java that allows users to interactively mine association rules from input Data. Also DBMiner, a data mining software tool, has been used for applying classification techniques. Loan assets are classified into Standard, Substandard (NPA) and Doubtful based on overdues. Association rules are presented in the form "in 80% cases, if an individual's Net Salary is between 0~5000 and Age is between 40~50, then that loan is considered as a Non-Performing Asset (NPA)".

Classification analyses a set of training data (i.e., a set of objects whose class label is known) and constructs a model for each class based on the features in the data. A set of classification rules generated by such a classification process can be used for better understanding of future data. In this application, classification process is used to classify loans based on the features in the data and help predict the kind of borrower behaviour based on the knowledge gained from the past data on borrowers.

The results obtained by mining the data are quite outstanding and provide a deep insight into the model constructed using the available data. The Mining tools used in this application explore the huge hidden information that is largely helpful, like evolving a set of characteristics of prospective borrowers with a high probability of default.

Working Papers

The Institute has come out with four Working Papers as follows:

W.P No 1: Technology Based Distance Learning : " New Vistas For Banks" - By Ms. V. Radha, Dr. V. P. Gulati and Shri. K. R. Ganapathy

W.P No 2: Construction of Security Policy for Banks - By Dr.V. P. Gulati, Shri. K. R. Ganapathy, Dr. Ashutosh Saxena & Shri. M.V.S. Prasad

W.P No 3: Electronic Commerce and Banks in India - By Dr.V. P. Gulati, Shri. K. R. Ganapathy, Dr. Ashutosh Saxena & Shri. M.V.S. Prasad

W.P No 4: An Approach To Establish Data Warehouse for Banks In India - By Dr.P. Radhakrishna.

Those interested in having a copy of these Working Papers may write to us or send their requests through email.

Awareness Series :

Public Key Infrastructures and Digital Certificates

Dr. Ashutosh Saxena, Faculty, IDRBT.

Security in computing is a very important issue. It is an area that deserves study by computer professionals, managers and even many computer users. The target of a crime involving computers may be any piece of the computing system. A computing system is a collection of hardware, software, storage media, data and people that an organization uses to do computing tasks. Whereas the obvious target of a bank robbery is cash, a list of names and addresses of depositors might be valuable to a competing bank. The list might be on paper, recorded on a magnetic medium, stored in internal computer memory or transmitted electronically across a medium such as a telephone line. The variety of targets makes computer security difficult. In any security system, the weakest point is the most serious vulnerability. In Security, an exposure is a form of possible loss or harm in a computing system; examples of exposures are unauthorized disclosure of data, modification of data or denial of legitimate access of computing. A vulnerability is a weakness in the security system that might be exploited to cause loss or harm. A person who exploits a vulnerability perpetrates an attack on the system. Threats to computing systems are circumstances that have the potential to cause loss or harm; human attacks are examples of threats, as are natural disasters, inadvertent human errors, and internal hardware or software flaws. Finally, a control is a protective measure - an action, device, procedure or technique - that reduces vulnerability.

The major assets of computing systems are hardware, software and data. There are four kinds of threats to the security of a computing system: interruption, interception, modification and fabrication. In an interruption, an asset of the system becomes lost, unavailable or unusable. An interception means that some unauthorized party has gained access to an asset. If an unauthorized party not only accesses but tampers with an asset, the threat is a modification. Finally, an unauthorized party might fabricate counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes, these additions can be detected as forgeries, but if skilfully done, they are virtually indistinguishable from the real thing.

Security Goals

Computer security consists of maintaining three characteristics: confidentiality, integrity and availability.

Confidentiality means that the assets of a computing system are accessible only by authorized parties. The type of access allowed to them is also specified like reading or viewing, modifying, printing or even just knowing the existence of an object. Confidentiality is sometimes called secrecy or privacy.

Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting and creating.

Availability means that assets are accessible to authorized parties. An authorized party should not be prevented from accessing objects to which he, she, or it has legitimate access.

These three goals make up security in computing. These three qualities can overlap and they can even be mutually exclusive. (For example, strong protection of confidentiality can severely restrict availability.)

Encryption provides confidentiality for data. Additionally, encryption can be used to achieve integrity because data that cannot be read generally also cannot be changed in a meaningful manner. Encryption is at the heart of methods for ensuring all three goals of computer security. Encryption is an important tool in computer security but one should not overrate its importance. Users must understand that encryption does not solve all computer security problems. Furthermore, if encryption is not used properly, it may have no effect on security or could, in fact, degrade the performance of the entire system. Weak encryption can actually be worse than no encryption because it gives an unwarranted sense of security. Thus, it is important to know the situations in which encryption is useful and to use it effectively. Encryption is a means of maintaining secure data in an insecure environment. Encryption is probably the most fundamental building block of secure computing.

Some encryption algorithms use a key K so that the cipher text message depends both on the original plain text message and the key value denoted by C=E(K,P). Essentially, E is a set of encryption algorithms, and the key K selects one specific algorithm.

Sometimes the encryption and decryption keys are the same, so that P=D(K,E(K,P)). This style of encryption is called symmetric encryption because D and E are mirror-image processes. In other cases encryption and decryption keys come in pairs. Then a decryption key, KD, inverts the encryption of key KE so that P=D(KD, E(KE,P)). Encryption algorithms of this form are called asymmetric, because converting C back to P is not just reversing the steps of E.

Using applied cryptography, PKIs govern the distribution and management of cryptographic keys and digital certificates that allow us to take advantage of several fundamental features:

- Confidentiality of information assures users that their communications are safe and readable only by the intended recipients. Message encryption using digital certificates assures this confidentiality.

- Integrity of data guarantees that message contents are not altered during the transmission between the originator and the recipient. PKIs provide for digital signatures to ensure the integrity of all transmitted information
- User authentication enables systems and applications to verify that users are who they claim they are and have the authority to access the resource. PKIs use digital signatures and user certificates to assure the authentication of all end entities and system resources.
- Non-repudiation prevents users of the PKI from denying that they have participated in a transaction or sent a message to another user or resource. With a legitimate digital signature in hand and the legitimate digital certificate that accompanies it, the chance that a message is forged or originated elsewhere approaches zero.
- System interoperability -- due to strict standards compliance -- enables a PKI's operation across a variety of hardware and software systems without any system-specific configuration requirements.

Effective PKIs are based on the Public Key Cryptographic Standards (PKCS), a family of standards which include:

- RSA encryption for the construction of digital signatures and digital envelopes.
- Diffie-Hellman key agreements that define how two people, with no prior arrangements, can agree on a shared secret key that is known only between them and used for future encrypted communications.
- Password based encryption hides private keys when transferring them between computer systems, sometimes required under Public-Private Key Cryptography.
- Extended certificate syntax permits the addition of extensions to standard X.509 digital certificates. These extensions add information such as certificate usage policies, other identifying information, etc.
- Cryptographic message syntax describes how to apply cryptography to related data, including digital signatures and digital envelopes.
- Private-key information syntax describes how to include a private key along with algorithm information and a set of attributes to offer a simple way of establishing trust in information provided.
- Certification request syntax describes the rules and sets of attributes needed for a certificate request from a certificate authority.

Recall that a digital certificate binds a previously-authenticated private key holder (a person) to the public key that accompanies it. This attestation, performed by a trusted party, creates a message containing the person's identification information, his or her public key, certificate usage rules, and other information. This message is then signed using the CA's private key and returned to the private-key holder. PKI hierarchies of trust use this concept to manage the public keys for all users, internal and external. With a PKI in place, a "Tree of Trust" is formed to represent how Certificate Authorities control certain aspects of other Certificate Authorities in the branches below them. Constructing this tree is one of the first activities in developing a PKI and is embodied in the Certificate Practices Statement (CPS) discussed later.

Certificate Management by Certificate Authorities

Key and certificate management are not tasks to be taken lightly nor are they for the faint-hearted. Extremely tight security is an imperative to maintain the trust that PKIs require. In essence, CAs provide 3 basic services to the entities (other CAs or end-entities) directly below them in the tree:

- Certificate Issuance
- Certificate Renewal
- Certificate Revocation

Root Certificate Authority

The highest level or root of the hierarchy of trust is the Root Certificate Authority. It is normally maintained off-line and only accessed when needed for signing purposes. Root CA responsibilities also include the generation and distribution of the Certificate Revocation List (CRL) in case of any private key compromise in the branches directly below the root. All these Root Certificates are self-signed. Their presence is required for validating a PKI certificate chain. Enterprise root certificates will normally be embedded in the Web browsers used to access PKI-protected resources. In the case of most cards used for various functions such as credit, debit and preloaded cards the hierarchical structure of CAs will be useful only when the volumes of these cards and transactions carried out through them are so large that a single CA cannot administer the key management and other issues. In such a scenario as an illustration each bank may become a CA under the overall supervision of an All India CA for Banks and Financial institutions like IDRBT/RBI on INFINET.

Certificate Revocation List (CRL)

The idea behind CRLs is to stop the uses of any digital certificates that are related to a set of private keys that were compromised (stolen). If a thief gains a copy of a private key and possesses its accompanying certificate, he has essentially stolen the identity of the private key holder. If the theft is not detected, the thief could use the key-pair (certificate and private key) to either: (a) masquerade as the legitimate key holder without any suspicion or (b) he could use the private key to sign forged certificates (if a CA key was stolen). Once a theft or compromise is detected, it is critical that the CA, which signed the key-pair, knows about it and places the certificate's serial number on the Certificate Revocation List immediately and re-publishes the list.

CRLs are defined by the X.509 Standard for publication and distribution of the identity of revoked, unexpired certificates. CRLs are composed of the serial numbers for all revoked certificates, with the CA that signed those certificates responsible for its near real-time maintenance to prevent any fraud or abuses using compromised private keys.

Protection of Keys

Protecting the private keys that are tied to a digital certificate's public key, especially those keys that are used to sign lower-level digital certificates, is very serious business under any PKI uses. Without this protection, the notion of any trust goes out of the window and the infrastructure will inevitably fail.

Stolen (copied) private keys from any end entity could be used to transact or communicate without any cause for suspicion. It is the same as a stolen identity, where a thief masquerades as the legitimate key-holder without any reasons to suspect wrongdoing. Similarly, if the keys for a Certificate Authority were compromised, the repercussions could be severe. With a stolen (copied) CA key in hand, a would-be forger could issue bogus certificates without leaving any clue to detect the forgery. Protection of all CA keys is absolutely critical to maintain the PKI's level of trust.

The more a private key is used to sign messages, the more instances a would-be attacker can obtain it for cryptanalysis. If these keys are changed often and regularly and managed well, they will remain safe from all forms of attack.

PKI cryptographic keys are extremely sophisticated in deterring would-be cryptosystem attackers. Because of its robustness, it is not really worth the effort to try breaking the cryptography. Even with all the computers on the planet working in tandem, an attacker would still find a tough time in reverse engineering or attempting brute-force methods (trying all possible combinations of a key) in determining the key. CAs will normally guard against such attacks anyway by using extremely long keys. They will also change their keys regularly and re-issue new certificates whenever they do so. Rather than trying to discover the key, thieves are better off trying to steal the actual key from where it is stored, so extra precautions must be taken to assure this cannot happen. Because CAs clearly understand the value of the keys in their possession they go out of their way to keep them safe from all possible attacks, physical and logical.

Every end-user or entity under a PKI is responsible for the safety of their own keys and certificates. This is the central theme and cannot be over-emphasized. A PKI's ability to guarantee assurances of authentication, message integrity, privacy and security cannot be realized once keys get into the wrong hands.

Note: We invite contributions from our readers on specific areas of banking technology for publication. Case studies are also welcome.

- 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 : 3534981-984 (4 lines), Fax : (040) - 3535157, 3536361
e-mail : publisher@idrbt.com , Website:http//www.idrbt.com