INTRODUCTION

Name of the Center: Prabhu Goel Research Centre for Computer & Internet Security

Location: HR Kadim Diwan Building, IIT-Kanpur

Lead person: Dr. Rajat Moona (Head)

Members of the team:

- Navpreet Singh, Associate Head
- Manindra Aggarwal, Professor
- Arnab Bhattacharya, Assistant Professor
- Dheeraj Sanghi, Professor (On leave)
- Prashant Srivastava
- Satyam Sharma
- Abhay Khoje
- Salih KA

Project number with DORD: END/PGC/CS/20020260

Date of creation: March 2003

Signature of the coordinator

Date: September 15, 2008

OBJECTIVES

The Prabhu Goel Research Centre for Computer and Internet Security at IIT Kanpur was established by Dr. Prabhu Goel with a generous grant of US$ 1million. Dr. Prabhu Goel, an alumnus of IIT Kanpur, is an active philanthropist and a highly successful private venture investor. He has founded several companies including Gateway Design Automation (acquired by Cadence), Frontline Design Automation (acquired by Avant Corporation), iPolicy Networks etc.

He established Poonam and Prabhu Goel Chair in the department of CSE (Computer Science and Engineering), IIT Kanpur. The centre was inaugurated on (June 3, 2003) by Dr. Vidyasagar, Executive Vice President, Advanced Technology Centre, TCS Hyderabad.

The vision of the centre is to become the nodal R&D centre in the country for all aspects of computer and Internet security. The charter of the centre is to help and educate various governmental and non-governmental organizations on security issues. The centre undertakes research, training and consulting activities, and collaborates with defense and security agencies in developing various security technologies.

In order to increase the security awareness, the centre holds short term training courses. The centre has conducted several intensive training courses on computer security and undertakes consulting activities for design of security policies, networks and other secure information systems.

IIT Kanpur regularly offers elective courses on cryptography and data security. The centre has augmented these courses with knowledge base on computer and Internet security. These courses are now available to senior undergraduate and post-graduate

students. As the centre evolves and activities grow in the area of security, we will also consider starting a Computer Security stream in the Computer Science MTech programme. In order to interact with other researchers working in the security area in the country and abroad, we plan to conduct regular visits, joint projects, and organize relevant conferences or workshops regularly.

CURRENT ACTIVITIES

The centre is currently undertaking the following activities.

- Academic courses for undergraduate and postgraduate programs
- Short term courses for industry and other organizations
- Postgraduate thesis work and undergraduate project work
- Workshops and conferences in the area of data security
- Various research projects
- Interactions with researchers in the area of security

Academic courses for undergraduate and postgraduate programs

Various security-related courses are being offered to the undergraduate and postgraduate students through the centre.

Short term courses for industry and other organizations

We organize short term courses for the industry and other organizations on a regular basis. A strong emphasis is laid on the practical aspects of information security in addition to the regular topics.

Postgraduate thesis work and undergraduate project work

The centre supports postgraduate thesis and undergraduate project work. Currently, we have four master's students pursuing their postgraduate thesis, supported by the Centre.

Workshops and conferences in the area of data security

The centre is organizing Hack.in 2009 - a workshop on computer and Internet security during March 17-19, 2009. This will involve participation from active researchers in the area of data security across the country.

Various research projects

Some of the current research projects under the centre include TransCrypt (an encrypting file system) and SCOSTA (a Smart Card OS standard) are being pursued vigorously in the Centre.

Interactions with researchers in the area of security

The centre regularly invites researchers in the area of security from other places and arranges talks and seminars by them. Prof. David Kotz from Dartmouth College USA shall be visiting the centre next on September 22, 2008.

RESEARCH PROFILE

List of Papers

Some of the recently published papers are as follows:

- K. V. Arya and P. Gupta, **Registration Algorithm for Motion Blurred Images**, The 6th International Conference on Advances in Pattern Recognition (ICAPR 2007), Kolkata, India, 2007

- Saeeduddin Ansari and P Gupta, **Localization of Ear Using Outer Helix Curve of the Ear**, International Conference on Computing: Theory and Applications (ICCTA), Kolkata, India, 2007

- Anupam Sana, Phalguni Gupta and Ruma Purkait, **Ear Biometrics: A New Approach**, International Conference on Advances in Pattern Recognition (ICAPR), Kolkata, India, 2007

- Satyam Sharma, Rajat Moona and Dheeraj Sanghi, **Transcrypt: A Secure and Transparent Encrypting File System for Enterprises**, Proceedings of the 8th International Symposium on Systems and Information Security (SSI 2006), Sao Paulo, Brazil, November 8-10, 2006.

- Dasari Shailaja and Phalguni Gupta, **A Simple Geometric Approach for Ear Recognition**, 9th International Conference on Information Technology (CIT), Bhubaneswar, India, 2006

- Hunny Mehrotra, Ajita Rattani and Phalguni Gupta, **Fusion of Iris and Fingerprint Biometric For Recognition**, International

Conference on Signal and Image Processing (ICSIP), Karnataka, India, 2006

- Nikunj Kela, Ajita Rattani and Phalguni Gupta, **An Illumination Invariant Face Recognition System**, IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), New York, USA, 2006

- P. Gupta, H. Mehrotra, A. Rattani, A. Chatterjee and A.K. Kaushik, **Iris Recognition using Corner Detection**, 23rd International Biometric Conference, Montreal, Canada, 2006

- Phalguni Gupta, Ajita Rattani, Hunny Mehrotra and Anil Kumar Kaushik, **Multimodal Biometrics System for Efficient Human Recognition**, In Proceedings of SPIE 'Defense and security symposium', Florida, USA, 2006

- Ajita Rattani, Nitin Agarwal, Hunny Mehrotra and P. Gupta, **An Efficient fusion based classifier**, In Proceedings of Workshop on Computer Vision, Graphics, and Image Processing (WCVGIP), Hyderabad, India, 2006

- R. Lokhande, K. V. Arya and P. Gupta, **Identification of Parameters and Restoration of Motion Blur Images**, Proc. The 2006 ACM Symposium on Applied Computing, pp. 301-305, Dijon, France, 2006.

- Manindra Agrawal, Nitin Saxena, **Equivalence of F-algebras and Cubic Forms**. STACS 2006, LNCS 3884: 115-126

- Ashish Agarwal, Pankaj Jalote, **Monitoring the Security Health of Software Systems**, Proceedings of the The 17th IEEE International Symposium on Software Reliability Engineering,Raleigh, North Carolina, USA (ISSRE 2006), Raleigh, North Carolina, November 7-10, 2006
- Prithwijit Guha, Arindam Biswas, Amitabha Mukerjee, P. Sateesh and K.S. Venkatesh, **Surveillance Video Mining**, Proceedings of the Third International Conference on Visual Information Engineering, Bangalore (India), September 26-28, 2006
- Arindam Biswas, Prithwijit Guha, Amitabha Mukerjee and K.S. Venkatesh, **Intrusion Detection and Tracking with Pan-Tilt Cameras**, Proceedings of the Third International Conference on Visual Information Engineering, Bangalore (India), September 26-28, 2006
- Ashish Agarwal, Pankaj Jalote, **Integrating static and dynamic analysis for detecting vulnerabilities**, Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC '06), Chicago, September 17-21, 2006.
- Prithwijit Guha, Amitabha Mukerjee and K.S. Venkatesh, **Appearance Based Multi-Agent Tracking Under Complex Occlusions**, Proceedings of the 9'th Pacific Rim International Conference on Artificial Intelligence (PRICAI), Lecture Notes in Computer Science (LNCS), Vol. 4099, Springer, pp. 593-602, Guilin (China), August 7-11, 2006.

- Navpreet Singh, Megha Jain, Payas Gupta & Shikha Bansal, **Network Monitoring Tool to Identify Malware Infected Computers**,AUUG 2006, Melbourne, Australia.
- Prithwijit Guha, Arindam Biswas, Amitabha Mukerjee and K.S. Venkatesh, **Occlusion Sequence Mining for Complex Multi-Agent Activity Discovery**, Proceedings of The Sixth IEEE International Workshop on Visual Surveillance (In conjunction with ECCV 2006), pp. 33-40, Graz (Austria), 13'th May, 2006.
- Brajesh Pande, Dheeraj Sanghi, Deepak Gupta, **Application Layer and In-Kernel Packet Filtering in the Network Monitoring Tool PickPacket**, Proceedings of Second International Conference on Global E-Security(ICGeS), UeL Docklands, April 20-22, 2006.
- Prithwijit Guha, Dibyendu Palai, K.S. Venkatesh and Amitabha Mukerjee, **A Multiscale Co-linearity Statistic Based Approach to Robust Background Modeling**, Proceedings of the 7'th Asian Conference on Computer Vision (ACCV), Lecture Notes in Computer Science (LNCS), Vol. 3851, Springer, pp. 297-306, Hyderabad (India), January 13-16, 2006.
- Prithwijit Guha, Amitabha Mukerjee and K.S. Venkatesh, **Efficient Occlusion Handling for Multiple Agent Tracking by Reasoning with Surveillance Event Primitives**, Proceedings of The Second Joint IEEE International Workshop on Visual Surveillance and Performance Evaluation of Tracking and Surveillance (In conjunction with ICCV 2005), pp. 49-56, Beijing (China), October 15-16, 2005.
- Brajesh Pande, Deepak Gupta, Dheeraj Sanghi, Sanjay Kumar Jain, **A Network Monitoring Tool- Pickpacket**, Proceedings of Third International Conference on Information Technology and

Applications (ICITA'05) Volume 2 pp. 191-196, Sydney, July 4-7, 2005.

PhD Theses

Title: Morphisms of Rings and Applications to Complexity
Author: Nitin Saxena
Supervisor: Dr. Manindra Agrawal
Date: June 2006

Title: Derandomazing Some Number-theoretic and Algebraic Algorithms
Author: Neeraj Kayal
Supervisor: Dr. Manindra Agrawal
Date: August 2006

M. Tech. Theses

Title: File System Independent Metadata Organization for Transcrypt
Author: Arun Raghavan
Supervisor: Dr. Rajat Moona, Dr. Dheeraj Sanghi
Date: June 2008

Title: A Device Mapper based Encryption Layer for Transcrypt
Author: Sainath S Vellal
Supervisor: Dr. Rajat Moona, Dr. Dheeraj Sanghi
Date: June 2008

Title: Scale and Affine Invariant(SAI) Descriptors for Matching Color Images
Author: V Apoorva Reddy
Supervisor: Dr. K.S. Venkatesh
Date: July 2007

Title: Perceptual Watermarking of Digital Video using the Variable Temporal Length 3D-DCT
Author: Vivek Kumar Agrawal
Supervisor: Dr. Sumana Gupta
Date: June 2007

Title: Key Management for Transcrypt
Author: Abhijit Bagri
Supervisor: Dr. Rajat Moona, Dr. Dheeraj Sanghi
Date: May 2007

Title: TCP Stream Reassembly and Web based GUI for Sachet IDS
Author: Palak Agarwal
Supervisor: Dr. Dheeraj Sanghi
Date: February 2007

Title: Design of a Hand Geometry Based Recognition System
Author: Saraf Ashish
Supervisor: Dr. Phalguni Gupta
Date: Jan 2007

Title: TransCrypt: Design of a Secure and Transparent Encrypting File System
Author: Satyam Sharma
Supervisor: Dr. Rajat Moona, Dr. Dheeraj Sanghi
Date: August 2006

Title: Multi-Agent Tracking Under Occlusion and 3D Motion Interpretation
Author: Pabboju Sateesh Kumar
Supervisor: Amitabha Mukerjee
Date: August 2006

Title: Secure Video Conferencing for Web Based Security Surveillance System
Author: Gurmeet Singh
Supervisor: Dr. T.V. Prabhakar
Date: July 2006

Title: Personal Identification Based on Handwriting
Author: Sachin Kumar Mangal
Supervisor: Dr. Phalguni Gupta
Date: July 2006

Title: A Novel Approach to Invariant Object Recognition
Author: Sravanthi Penmetsa
Supervisor: Dr. Phalguni Gupta
Date: July 2006

Title: A Simple Geometric Approach for Ear Recognition
Author: Dasari Naga Shailaja

Supervisor: Dr. Phalguni Gupta
Date: July 2006

Title: Intrusion Prevention and Automated Response in Sachet IDS
Author: Chinmay Niranjan Asarawala
Supervisor: Dr. Dheeraj Sanghi
Date: May 2006

Title: Reconstruction of Web Based Email in PickPacket
Author: Vinaya Natrajan
Supervisor: Dr. Dheeraj Sanghi
Date: May 2006

Title: Supporting IPv6 in PickPacket
Author: Devendar Bureddy
Supervisor: Dr. Dheeraj Sanghi
Date: May 2006

Title: Improving the Security of Software Applications
Author: Ashish Aggarwal
Supervisor: Dr. Pankaj Jalote
Date: May 2006

Title: Human Activity Representation, Analysis and Recognition
Author: Hedau Varsha Chandrashekhar
Supervisor: Dr. K.S. Venkatesh
Date: May 2006

BTech Projects and other Minor Research reports

Title: A Kernelspace Public Key Infrastucture for TransCrypt
Author: V Bhanu Chandra
Supervisor: Dr. Dheeraj Sanghi, Dr. Rajat Moona
Date: May 2007

Title: A daemon for secure smart card support in the encrypted file system Transcrypt
Author: Deeptanshu Shukla
Supervisor: Dr. Dheeraj Sanghi, Dr. Rajat Moona
Date: April 2007

Title: PickPacket: A Distributed Parallel Architecture
Author: Dungara Ram Choudhary

Supervisor: Dr. Dheeraj Sanghi
Date: May 2006

Research projects

The Prabhu Goel Research Centre for Computer & Internet Security has undertaken several computer security related projects including the following.

- Transcrypt
- MIDS- Malware Infection Detection System
- Sachet - Intrusion Detection System (IDS)
- PickPacket for Gigabit Networks
- Cryptanalysis
- Netlog Server
- Secure Linux
- Trinetra & Indra Encryption Algorithms
- SCOSTA

Transcrypt

TransCrypt is a kernel-space encrypting file system that incorporates an advanced key management scheme to provide a high grade of security while remaining transparent and easily usable. TransCrypt makes a crucial distinction between the kernel and user-space from a security perspective. It excludes the superuser account or any user space process from the trust model. TransCrypt to assume a wider threat model than that tackled by existing systems

and making it immune to several attacks that may be launched from the inside.

TransCrypt provides file level and user level granularity during encryption. It provides a number of security options to fit into an individual's security model.

MIDS- Malware Infection Detection System

This tool monitors the network traffic and identifies all the (active) computers on the network which are infected with any kind of Malware. It provide the IP address, MAC Address and type of infection for the all the identified hosts. This is a freeware tool which works on Linux.

Tcpdump is used to take a trace of the network traffic and shell scripts are used to analyse the collected data. Signature packets in the collected traces are used to identify the type of infection. Several configuration parameters can be set as per requirement.

The tool can be installed on any Linux machine. To identify the infected hosts on any Subnet/VLAN, the traffic needs to be monitored on the mirror port of the Default Gateway for that Subnet/VLAN.

We have been using this tool at IIT Kanpur. IIT Kanpur is a premier Academic Institute of India. IITK has a LAN with more than 6500 nodes. This tool is regularly used to identify infected machines on the Campus

LAN. The administrators of the infected machines are informed and in case appropriate action is not taken by the administrator, the machine is disconnected from the network.

We have currently developed MIDS-10 system. We are in the process of developing MIDS-100, MIDS-200 & MIDS-400 systems.

Sachet - Intrusion Detection System (IDS)

This is a network based IDS with a distributed architecture and centralized control. A signature based packet analyzer runs on different machines in the network and generates an alert. An agent running along with the packet analyzer sends these alerts to a central command console for further analysis. The console also logs these alerts to a database.

The entire system can be controlled and configured from the central console. The signature data base at each agent can be changed on the fly and the packet analyzer can be started and stopped from the console. The agents communicate with the console using the same underlying network. All communication between agents and console is encrypted and the agents authenticate with the console before sending alerts or accepting commands from the console.

The agents do not communicate among themselves. The central console has a command line interface as well as a web based GUI interface. Thus it is possible to control the console from a remote location through a browser. The GUI has facilities to control the agents and to retrieve old information from the alert database.

PickPacket for Gigabit Networks

PickPacket is a network monitoring tool that can filter packets based on the IP addresses, port numbers and the application layer data present in these packets. It consists of four components. They are

- PickPacket Configuration File Generator:- This component is used to generate configuration file that contains the filtering criteria.
- PickPacket Filter:- This component captures packets according to the criteria specified in the configuration file and stores them on a storage device.
- PickPacket Post Processor:- This component analyses the data captured by the filter by separating this data into individual connections.
- PickPacket Data Viewer:- This component shows the result of capture in a user friendly manner.

PickPacket Filter is responsible for capturing and filtering the packets transmitted on the network at the same time as they are transmitted. Other components will work offline after filter collects live packets from the network. So, performance of the filter is crucial for the successful working of PickPacket.

Cryptanalysis

Undertaking basic research in Computer Security is one of the main goals of the centre. We have already done some work in this area. A major breakthrough was achieved when it was proved that primality testing can be done in polynomial time. This result is of tremendous theoretical significance. It is also of importance in cryptography since several cryptographic algorithms require the generation of large prime numbers.

The goal of the cryptanalysis is to identify the algorithm used to obtain a given cipher stream. The work already done includes differentiating between DES, AES, IDEA and RSA. A number of techniques have been developed, and at the moment, given a

cipher text of size around 4KB, the correct algorithm can be identified with at least 75% accuracy. (In case of RSA, the accuracy is more than 95%).

Work on cryptanalysis of encrypted speech has also been attempted. The problem here is to decrypt a given encrypted speech stream, encrypted by a stream cipher whose keys keep changing frequently. Preliminary work has been done here. Under the assumption that the stream is encrypted by a single LFSR-based cipher, speech can be partially decrypted, we can identify zones in the speech that correspond to spoken words and gaps between words.

Netlog Server

This is a new project on which we are working. This is a tool which can be run on any application server or can be installed on a Linux Server. It captures all the traffic and stores it in a mysql database. The collected data can be used at a later stage for forensic analysis. A PHP based front end is being developed for helping in the analysis of the traffic.

Secure Linux

The problem of computer security is not new. It was of importance even before computers entered our lives. Although the parameters were different then, the fundamental principles involved haven't changed much.

Our project aims to build a secure Linux. We have studied the known security problems in standard Linux. The standard Linux kernel provides Discretionary Access Control, which is not secure enough

for many domains like military agencies. It also leaves the system very vulnerable to damage caused by a single malicious or buggy application. We aim to provide a Mandatory Access Control mechanism in Linux. We are studying various theoretical Access Control Models proposed over the years.

We are also looking at existing Unix/Linux systems which provide additional security. These include Security Enhanced Linux provided by US National Security Agency, and TrustedBSD. We are investigating the access control models used by these systems, and how the abstract notions map to an actual Linux system. For our secure linux, we may propose a new security model, or modify and combine existing models. We want that the system's security policy should be flexible and configurable, yet efficient and easily manageable.

TIED, LibsafePlus: The complete buffer overflow solution

TIED and LibsafePlus can be used for protecting vulnerable C programs from buffer overflow vulnerabilities. The tools have been tested and found to be effective against all known forms of buffer overflow attacks which occur due to the incautious use of C library functions such as strcpy(). We hope that this would help the computing community in their search of an efficient and exhaustive solution for one of the most commonly exploited form of attack.

Trinetra and Indra

Trinetra is a new symmetric key cryptography algorithm, was designed at IIT Kanpur. It is a modern computer based code language system, which can digitize long, alphabetic messages within seconds. Indra is another symmetric key cryptography

algorithm. This algorithm is currently in the testing phase prior to deployment.

SCOSTA

In order to standardize and secure the data of the Transport department (MoRTH), Govt. of India, deployed the smart card technology for Indian Driving Licenses and Vehicle Registration Certificates (both for commercial and private use vehicles).

A technical Sub-committee was set up to draw operating system specifications for the smart card based Indian Driving Licenses (DL) and Vehicle Registration Certificates (RC) on in June 2001. The SCOSTA specifications were defined by this committee. The SCOSTA specification is largely compliant with the international ISO 7816 standard (parts 4 to 9) for smart cards.

The specifications drawn for the operating system, key management system, application and card layout and ISO definitions are mandatory to be complied with and form an integral part of SCOSTA and DL/RC applications. In addition, the cards for use with these applications must comply with the ISO 7816 standard (parts 1 to 3) that detail the electrical, physical, and communication aspects for smart cards.

All specifications are open and can be downloaded from www.scosta.gov.in

The SCOSTA project was originally initiated with the following principal objectives.

Standardization of Information

The card layout, data fields and other relevant information stored on the card is uniform and can be read and written all over the country.

Inter-operability

Since the Indian Driving License and Vehicle Registration Certificate are to be deployed nationwide, it is essential for the standards to be interoperable. SCOSTA specifications deal fully with this aspect.

Multi Vendor, Non-Proprietary Open Architecture

Keeping in view the need for future up-gradation, multi vendor support and the critical requirement of the specifications and product to be non-proprietary, it is essential to have the operating system specification to be open and standard.

Security and Integrity of Data

A microprocessor based smart card can ensure that only authorized persons can read or write the application data stored in the card. SCOSTA supports both password-based and key-based authentication of users. The DL and RC application specifications both include secure key management systems that ensure that only officials authorized to change the card data can do so and that it is not possible to create forged DL and RC cards.

SIGNIFICANT ACHIEVEMENTS

TransCrypt

TransCrypt is an enterprise-class encrypting file system. It uses strong cryptographic methods to protect your data against theft. TransCrypt is completely transparent — no changes to existing applications are required.

TransCrypt's primary strengths are:

- **Easy-to-use** sharing via the standard ACL interface
- **root is not trusted** in our threat model
- **Flexible** enough to accommodate various degrees of security depending on *your* requirements
- **Scalable** design

E-Passport

The Indian electronic passport is equipped with an electronic chip and an embedded antenna to interface in a contactless manner with the passport readers. The electronic chip runs an Operating System program which is a home grown standard known as SCOSTA-CL implemented by several reputed companies. The SCOSTA-CL standard is compliant to international civil aviation organization (ICAO) specified standard for reading passports across the world. However the Indian Passport standard goes one step ahead and defines the standard of interoperability even while personalizing the passports in the passport offices across the country and missions abroad. This permits the inlays with embedded chip and antenna to be procured by the manufacturers across the world without any further implication of security than what is required for a blank passport booklet.

The Indian Electronic Passport OS standard is defined by IIT Kanpur in collaboration with NIC New Delhi and members from the Smart Card Forum of India (SCAFI). The OS personalization software is developed by NIC New Delhi in consultation with IIT Kanpur. The ISP Nasik is the agency that manufactures the blank electronic passports with electronic chip inlays. The standard compliance testing procedures are established by STQC to test against the compliance to the SCOSTA-CL OS standard along with the IIT Kanpur and NIC New Delhi. The personalized full function electronic passports have been tested for inter-operability and have been found to function well and sometimes better than the passports available elsewhere in the world.

MAJOR CURRENT PROJECTS

- Transcrypt
- Biometrics Standards for e-governance
- SmartCard Applications
- SCOSTA: Smart Card Operating Systems Standard for the country
- SmartID: IIT Kanpur Secure ID Card and its applications
    - Student Attendance
    - Access Control System (ACS)
    - Library: Identification of user and self issue/return
    - Swimming Pool Application
    - Commands Library
    - Vending Applications
- The Indian Electronic Passport
- Readers Terminal for smartcards

Transcrypt

TransCrypt is an enterprise-class encrypting file system. It uses strong cryptographic methods to protect your data against theft. TransCrypt is completely transparent — no changes to existing applications are required.

TransCrypt's primary strengths are:

- **Easy-to-use** sharing via the standard ACL interface
- **root is not trusted** in our threat model
- **Flexible** enough to accommodate various degrees of security depending on *your* requirements
- **Scalable** design

Currrently, TransCrypt has been implemented on Linux as a layer over the ext3 file system. All the code is available, free of cost, under appropriate open source licenses.

Biometric Standards for e-Governance in GOI

With the spread of electronic processing and communication, a number of applications based on "paper" are being moved to electronic format to improve the speed of transactions and ease of use. However, this transformation comes with its own set of issues; one of the most important being security. Therefore, in many applications, biometric data of the user is required to validate the identity of the user. There are a number of companies that offer biometric solutions; however, all of the solutions are proprietary. These are undesirable since using them ties one down to a single company forever. Therefore, there is a strong need to create open standards for biometric data usage in India. For this reason, the government (through NIC) has constituted a committee to devise a complete set of standards for biometric use in e-governance. This article describes the current biometric scenario and a strategy for creating the standards.

Types of Biometric Data

The most important type of biometric data is finger prints. The patterns on a fingerprint are good for identification and also are easy to obtain. Besides the fingerprints, iris image, facial features, and handwriting are also used. Fingerprints are stored in two different ways: as bitmap image and as minutiae elements. Minutiae elements are extracted from the image by analyzing the line patterns on the fingerprint. The advantage of minutiae is that it

requires very little storage. However, different companies extract different minutiae elements and are very secretive about it.

There does exist a worldwide standard for biometric data, created by International Organization for Standardization (ISO). It is documented in ISO 19784 and ISO 19794 (these documents are downloadable from ISO website http://www.iso.org against payment). However, these standards are not widely used. Firstly, the companies do not want to use them since they are not interested in interoperability. Secondly, there is no clarity about what type of biometric data should be used in different applications (one fingerprint or five or ten, only fingerprint or fingerprint with iris etc).

Our Approach

We plan to start with the ISO standards as baseline documents. They provide a reasonably comprehensive description of the way biometric data should be extracted, stored, and used. There are likely to be some points that will not be clear in the standards and we will need to fill these gaps by creating a suitable description of these.

Once the standards are defined completely, we will design algorithms that extract, store and use biometric data according to these standards. These algorithms will then act as benchmarks for algorithms and data supplied by any vendor.

We plan to approach this task in a stepwise manner. We will initially focus on the fingerprint data as it is the most important one and most of the applications use only this. For this, as described earlier, we need to create the standards for both bitmap and minutiae data. Of these, the minutiae data specification will be more involved (and more important as well; e.g., the National ID

project will be using the minutiae standard). The benchmark algorithms will be developed at IIT Kanpur and handed over to NIC for use.

Once the fingerprint specifications and algorithms are complete, we will move on to other forms, e.g., iris, handwriting etc. handling them in decreasing order of importance.

SMART ID CARD

The Smart ID cards contain relevant information about the card holder. The memory size of the chip inside the smart card is about 4 KB which contains minimum of 8 files of different sizes named as EF1 to EF8. User information is stored in these files and can be categorized as private or public. Public information (e.g. name, photograph, department, card expiry date etc.) is stored in files and is also some of them are printed on the Smart ID Card. Data of private nature, such as salary, PF number, PAN number, and account information etc., can be read/updated only by appropriate authority. The data is also password protected.

Smart ID cards are issued by the top authority (ID Cell) to the students and employees when they join the institute. There is provision to issue cards to dependants of students and staff as well. Each card has an expiry date and a valid till date. Although the expiry date is till the end of the program of a student, the valid till date is only till the end of semester. After registering for the next semester, the student needs to update the card to make it functional. The students who are terminated, cannot update their cards. So, though they are allowed to retain their ID cards, they cannot use it anywhere as it is expired. In case of an employee, the

expiry date of the card is the full tenure of the services of the employee.

Smart card-based ID systems offer significant benefits to the institute and the card holders. Even with the increase in the number of students, the process of issuing cards is now completed in just 2 days. The ID card is a multipurpose card. There is no need to issue different cards for library, swimming pool memberships etc.

All authentication and authorization mechanism are implemented using symmetric key cryptography. An interesting application of the Smart ID is that it can be used as an electronic purse in vending machines. Smart ID card can be loaded with prepaid cash, which can be used to dispense beverages and snacks at vending machines.

There are four levels of hierarchy in the smart card based ID system of IIT Kanpur. The ID Cell is at the highest level and has all the privileges. It creates and issues Smart ID cards to all users. The second in hierarchy is Application creation authority followed by verification authority and lastly the user card. The different levels of authority have different and varied access to the user cards. They are granted privileges with the help of various cryptographic keys.

Application creation authority can create different applications in the user card, for example, swimming pool application, vending application etc. Verification authority is only authorized to read certain data based on the permissions. For example, the office bearer at the Dean of Student's affairs may be allowed to see all the details of a student but not that of a staff whereas; the accounts section has access to the bank account number. They may have permission to just read data or also update it.

ID cell authority card can upgrade a user card to verification authority and then to ACA if needed. This ACA can even be upgraded to ID cell authority card.

Applications of Smart ID cards

The students and employees of IIT Kanpur are issued smart card based ID cards. These are multipurpose cards and are being used in various applications all over the campus. Apart from being used for identification, these cards are being used for marking attendance, as swimming pool membership cards, and as e-purse as well. Some of the applications implemented are listed below with a brief description.

Student Attendance

The ID card holders can mark their attendance with smartcards. Software has been built by the smartcard application group at IIT Kanpur which allows this conveniently. The user will inserts the smart ID card in the smart card reader at the terminal where attendance can be marked and present a finger for fingerprint verification. After successful verification, the attendance is marked. This application is running successfully in the Computer science Department. Here the Post graduate students are marking their attendance through this software. Recently it has been deployed at the Visitor's Hostel and Directorate office as well where it is being used to mark the attendance of the employees. Attendance records can be viewed by using a web based application called Attendance Management System.

Access Control System (ACS)

The smart ID cards can be loaded with access rights of the

individual to a particular building or lab or office. The doors need to be fitted with electronic door locks and smart card readers connected to a computer. On insertion of the smart ID card in the reader, the ACS software will read the access rights of the user and grant or deny access accordingly. Visitors can also be issued with visitor passes with their access rights. On leaving the building, the visitor will hand back his Access Card to the reception. In case the visitor does not return the card, it will not matter as the card will automatically become defunct after the date of validity. For added security and avoiding misuse of access rights, there is biometric verification as well.

Library: Identification of user and self issue/return

Identification of students and employees at the library can be done easily with smart ID cards.

A person can be thoroughly authenticated with an additional biometric information verification such as fingerprint. Once this has been established, then the person may be allowed to issue / return books without assistance from staff. Software to facilitate this authentication is ready and is now being integrated with libsys, the library management system being used by the Central Library at IIT Kanpur.

In self issue/return process, a user can issue and return books without any assistance from the staff.

Swimming Pool Application

The Smart ID Card has been extended to provide memberships to the swimming pool users. There is software to register members and write the membership information on cards. Another software called Swimming pool Front Desk software marks entry/exit of the members into the swimming pool. Logs of all entries and exits

on a daily basis are maintained. These logs can be viewed a friendly format. The software has been deployed at IITK swimming pool and is running successfully. Currently approximately more than 1000 unique memberships have been created among the students, staff and their dependents and more than 300 entry/exits are marked each day by the members.

Commands Library

Under this project a standard library in C++ has been developed which is in accordance with the ISO-7816 standards for smartcards and the PCSC API. This library abstracts the way data is passed to the Smart-Card OS by applications in T0, T1 and Raw protocols. The various features also include implementation of secure messaging and various Cryptographic algorithms (DES, Triple DES). The above protocols and features are being implemented in line with the SCOSTA standards (SCOSTA-CL1.2).

Vending Applications

The Smart Id cards can be loaded with pre-paid cash with the help of the vending application. This card can then be used dispense tea, coffee etc. from vending machines. One such coffee vending machine has been installed in the computer science department. The system is managed and maintained by the office staff /students on a no profit no loss basis. Thus it is hygienic, cheap and fast. The transaction is cashless. Users are encouraged to bring their own mugs so as to reduce the consumption of plastic cups. Thus it is environment friendly. The machine is always on and hence, the beverages are available round the clock.

The Indian Electronic Passport: A perspective

The Indian electronic passport is equipped with an electronic chip and an embedded antenna to interface in a contactless manner with the passport readers. The electronic chip runs an Operating System program which is a home grown standard known as SCOSTA-CL implemented by several reputed companies. The SCOSTA-CL standard is compliant to international civil aviation organization (ICAO) specified standard for reading passports across the world. However the Indian Passport standard goes one step ahead and defines the standard of interoperability even while personalizing the passports in the passport offices across the country and missions abroad. This permits the inlays with embedded chip and antenna to be procured by the manufacturers across the world without any further implication of security than what is required for a blank passport booklet.

The Indian Electronic Passport OS standard is defined by IIT Kanpur in collaboration with NIC New Delhi and members from the Smart Card Forum of India (SCAFI). The OS personalization software is developed by NIC New Delhi in consultation with IIT Kanpur. The ISP Nasik is the agency that manufactures the blank electronic passports with electronic chip inlays. The standard compliance testing procedures are established by STQC to test against the compliance to the SCOSTA-CL OS standard along with the IIT Kanpur and NIC New Delhi. The personalized full function electronic passports have been tested for inter-operability and have been found to function well and sometimes better than the passports available elsewhere in the world.

Readers Terminal for smartcards

Smart cards are commonly used for applications such as ID, loyalty, payment and security. With an earlier project under MCIT, IIT Kanpur and NIC together had been able to establish a standard for the Smart Card operating system called SCOSTA. The SCOSTA

standard is compliant to a set of ISO-7816 standards which are open standard for smart card interactions. SCOSTA and its updated version SCSOTA-CL have been used for the purposes of Driving License, Vehicle Registration Certificate, National ID, Electronic Passport etc. in India. It is being projected as a standard for the Indian Smart Card projects including the Rastriya Swastya Bima Yojna, National Rural Employment Guarantee Scheme etc.

The goal of SMART CARD READER AND TERMINAL STANDARDS project is to establish continuity with SCOSTA card definitions and to develop reader specifications for the hardware and the OS to support SCOSTA based applications. This project therefore aims as developing an open interface which might be used by the enforcing agencies and others who would like to operate with the SCOSTA and other similar smart cards for developing larger applications. Some of the desirable features in such a reader are the following.

(a) Seamless integration of various peripherals such as printers, network interface etc.

(b) Support for multiple smart card reader interfaces including contact and contact-less interfaces and card to card communication
and authentication.

(c) Abstraction of display to support text-only and text and graphics.

(d) Public key infrastructure to support encryption, decryption and authentication, digital certificates and digital signatures.

SCOSTA (Smart cards for transport applications)

In order to standardise and secure the data of the Transport department (MoRTH), Govt. of India, deployed the smart card

technology for Indian Driving Licences and Vehicle Registration Certificates (both for commercial and private use vehicles).

There have been two standards defined for SCOSTA.

1. SCOSTA standard was defined in 2002 with an aim to use it as an ID standard OS for the contact cards. The standard supports TDES algorithms for confidentiality, integrity and authentication.
2. SCOSTA-CL standard was defined in 2007 as an increment from the SCOSTA standard. This supports secure messaging and few other stronger mechanisms for confidentiality, integrity and authentication. It also includes session key establishment and is suitable for contact and contact-less operations.

The current research in SCOSTA area tries to define the SCOSTA standard with Public-key cryptography. This will be suitable for all applications of SCOSTA and SCOSTA-CL and will additionally support schemes such as digital signatures and e-cash. The system can be used for e-payment mechanisms as well as for other applications including national ID.

PRESENT FINANCIAL PROFILE

Statement of Accounts

Period: From 01-04-2008 to 04-09-2008

Details of Actual Expenditure

Serial Number	Budget Head	Amount(Rs.)
1	CONTG	42882
2	EQUIP	0
3	HON	5000
4	SALARY	376015
5	TA	250329
	Total	674226

Period: From 01-04-2007 to 31-03-2008

Details of Actual Expenditure

Serial Number	Budget Head	Amount(Rs.)
1	CONS	46188
2	CONTG	421526
3	EQUIP	2548533
4	HON	320000
5	SALARY	615766
6	TA	268470
	Total	4220483

PRESENT ADMINISTRATIVE PROFILE

The centre is presently headed by Dr. Rajat Moona. He is ably supported by Mr. Navpreet Singh as the Associate Head.

FUTURE COURSE OF ACTION

Our future course of action will span the following areas:

- Workshops
- Training
- Short term visitors
- Consultancy
- Staffing

Workshops

Workshops will be held regularly covering the area of computerand Internet security. The next workshop, Hack.in 2009 has been scheduled to be held during March 17-19, 2009.

Training

We intend to provide courses on security on a six monthly basis. This will include the latest security technologies. Generally, the over-worked network administrators are unable to understand the perspective of the malicious crackers (hackers) and hence are not able to come up with secure design of the network infrastructure.

In addition to the regular information, we also intend to provide comprehensive information related to Ethical Hacking, which is a method of using the same methods and tools as a regular cracker to hack into one's own network. This enables to identify and plug-in potential loopholes in the network before a malicious cracker does so. Needless to say, when augmented with regular security practices, this provides for a more comprehensive security posture.

Short term visitors

We will invite short term research personnel who will work on cutting-edge technologies. This will also enable the interaction with

peers, will result in Industry involvement, and enable us to forge a beneficial relationship with it.

Consultancy

We intend to develop this area as our core competency. This will include penetration testing and consultancy about comprehensive secure network design. This will prove beneficial to the organizations which will be able to gain more from our expertise in this area.

Staffing

As the activities of the centre are going to be increased manifold in the near future, we plan to hire more staff which will enable us to meet the demands of the increased activities of the centre.