

REGIONAL CYBER SECURITY RESEARCH CENTRE

Background & Justification:

The rapidly spreading use of computers and computer networks and the many advantages of open global network interconnections also have created increasing needs of improved information security. Software solutions and tools are irreplaceable cornerstones in network security. Network security software skills are a necessity, not only for IT and security specialists, but for every computer and computer network user. All this has profound implications on IT education, but also on all education, in which the use of computers and computer networks is inevitable. An interdependent network of information technology infrastructure called cyberspace, forms the backbone of all the information needs of all nations, but major potential applications are being hindered because of serious security and privacy concerns. A new type of threat called Cyber-terrorism has started influencing the Internet adversely. To improve the identified underlying issues, many organizations need to review as to how security risks, threats and costs are identified, measured and managed. Internet Security also has been a major concern, after various security breaches. Today, even after two and a half decades, the internet still remains vulnerable to a number of attacks. Many early network protocols that now form part of the internet infrastructure were designed without security in mind and hackers are continuously deploying more sophisticated and complex methods of attack. Hence it is very important to investigate and deploy procedures by which how security is implemented, in communication networks. Information infrastructures are an eclectic mix of open and closed networks, private and public systems, the Internet, and government, military, and civilian organizations. Significant efforts are required to provide infrastructure protection, increase cooperation between sectors, and identify points of responsibility. The threats to infrastructures are many, and are increasing daily: information warfare, hackers, terrorists, criminals, activists, and even competing organizations all pose significant threats that cannot be adequately dealt with using the current infrastructure model. Because of the need for new and different organizational infrastructures, management is has to reconsider its purpose and its methods of operation.

Information technology not only challenges and alters the way we produce new goods and services, but also triggers far-reaching change in institutional arrangements, social norms, and cultural values. It is playing a crucial role in our economic well being and results in a relationship among societies and nations never experienced before. Even educational institutions are being revolutionized through distance learning by the new computer-mediated communication technology and Internet-based support.

In addition to adjusting to these changes, societies will also have to come to terms with the unprecedented speed with which change occurs. This pace is accelerating, because increasingly powerful technologies facilitate the exponentially multiplying pool of knowledge and vice versa. Besides that the steadily growing international computer network user community needs an expanding staff of well educated network security professionals to guarantee the reliability of the global IT infrastructure of computer nodes in wired and wireless networks

RCSRC is a security research centre being setup at the Punjab Engineering College. The primary focus of RCSRC is to conduct high quality research in the general areas of security, and performance optimization in Networking, at affordable costs. The Centre will be a platform to provide defense against other threats such as information warfare. Our mission is to develop information infrastructures into more secure and reliable infrastructures and to enhance the communication networks and protocols of today's best-effort Internet.

The goal is to explore allied areas of networking, with the emphasis on verified designs, implementation, and evaluation of secure network systems, protocols, and applications. Institute research facilities include campus-wide wired and wireless networks as well as a heterogeneous collection of computing systems and some new infrastructure. In effect, PEC is an extensive test bed with several thousand wireless networked computers and active users.

VISION

Future communications networks, especially wireless networks, will be more robust, more powerful and more flexible in a wide variety of operating

environments, apart from being more vulnerable to cyber hacking resulting in more cyber security crimes. Hence, the urgent need to establish a Cyber Security Research Centre. The research work to be undertaken in the Cyber Security Research Centre and data collected here shall be of great benefit to the entire Research community. We aim at creating a technology rich environment conducive to constructive discussions and evolving thoughts which will lead to innovative ideas in unwiring and digitizing the world securely at affordable costs. The Vision for the RCSRC will to:

- Aid and advise organizations in cyber security policy enforcements, conduct of security audits and incident handling
- Provide various IT organizations, including the Police department, consultancy for design of secure networks including deployment of Security administration software like intrusion detection, management software for security software and vulnerability checking, protection against port scanners, password crackers etc
- Train manpower in the cyber security related skills needed by state departments including police, network users, IT professionals, and network security specialists. By taking the policy seriously and teaching all of the stakeholders about their role in maintaining it, they will embrace the policy as an integral part of their jobs.
- Facilitate research work for undergraduate and postgraduate students and researchers in the concerned areas
- Disseminate research results through journal and conference publications, technical reports, and public domain software.
- Create a digital knowledge library in the form of WEB/FTP server consisting of information in the above mentioned areas.
- Undertake projects with Government of India, Nasscom, IT Industry in collaboration with academia.
- Conduct interdisciplinary training programs for state departments, IT industry and academia.

Objectives to be achieved by RCSRC:

- Conduct high quality research in emerging areas of ICT especially cyber security, wireless mobile computing, and networking.

- Identify key research needs and active industry partners as a sustainable way to expand research capacity at the Punjab Engineering College with special emphasis on Cyber Crimes.
- Create an environment for graduate students to seek jobs closely aligned with their research interests or to remain in a research community supported by strong industrial relationships.
- Create innovative solutions via commercial applications of research.
- Create ongoing opportunities for the transfer of skills, knowledge, people and ideas between RCSRC and the community at large.
- Foster interdisciplinary research programs
- Partner other cyber research organizations
- Cultivating new secure technologies, that provide seamless networking between heterogeneous networks, to deliver connectivity at lower cost and higher bandwidth for increased productivity
- To maintain high quality of confidentiality and authentic solutions scalable for low-power devices in networks
- Safeguard security of campus network systems.

Key Areas identified for Research work by RCSRC:

- Design & developments of Secure Network Protocols & Algorithms
- Network and systems security protocols, Architecture & Performance Measurements & Analysis
- Low Cost Secure Wireless network & Mobile Communication & Converged Access Devices
- Wireless LAN Modeling, Analysis, Deployment & Testing
- Effectively Design technologies such as MANET, 802.11, 3G/4G, Ultra Wide Band, 802.16 and Bluetooth
- Development and deployment of cost-effective and relevant services in such areas as e-Governance, e-learning, telemedicine.
- Design and development of security administration software
- Network Monitoring, Biometric devices, Surveillance and Forensics through Intelligent traffic Analysis

Impact Envisaged:

The Emergence of Cyber Security Research Centre as a regional venue for communication, commerce, education and entertainment will blur traditional political and organizational boundaries, make time zones irrelevant and erase language barriers. A wide range of security technologies exists that provide solutions for securing network access and data transport mechanisms within the corporate network infrastructure. Many of the technologies overlap in solving problems that relate to ensuring user or device identity, data integrity, and data confidentiality. The intent is to develop an in-depth understanding amongst the various organizations of how these technologies can be implemented in corporate networks by designing and Implementation of the site specific Corporate Security Policy. The research and development in this area should be able to give outcomes that support advanced communications by developing and enhancing new generation technologies to escalate reliability, integrity, flexibility, security, and deliverance.

Rural development using digital technology also seems to offer great promise, but visionaries who have experimented with rural digital services have come across three major barriers to wide-spread deployment of digital technology. These barriers are connectivity, hardware cost, and authoring tools for user-appropriate content (e.g., content in local language including speech interfaces, and services). By focusing our research and development efforts on these problems of providing wireless connectivity, we can create an attractive market opportunity for rural services. To make this a reality there are several research problems in the areas of wireless communication and security that must be addressed to. These are:

- **Infrastructure Security:** Numerous problems exist in the protection of infrastructures. Aside from the obvious technical, legal, and financial aspects involved, there are also numerous misunderstandings between business and government over what protecting the infrastructure entails. This raises numerous concerns over liability, information sharing, and vulnerability issues that have been plaguing infrastructure protection since day one. By identifying these interdependencies a greater level of security can be provided for defending against such infrastructure attacks.

- **Wireless Antennae:** Reliable communication can be significantly enhanced by use of appropriate low-cost interoperable antennae.
- **Security:** Before widely deploying public WLANs, wireless carriers and service providers must overcome security flaws. The ability to reliably identify message sources, destinations, and identification of users is key issues, which needs integration and application of biometrics and secure authentication mechanisms.
- **Network configuration and protocols:** The ability to achieve efficient and reliable message routing depends on routing protocols that take into account the network topology, message characteristics, and link capacity.
- **Quality of Service:** Streaming media present a particular challenge to ad hoc pack switched networks. Protocols must be developed that provide the best possible service under the various conditions.
- **Operating system:** The need to support software radio, specialized sensors, and ad-hoc networking argues for a real-time OS. The need to minimize cost implies a microkernel OS that may not support common PC functionality. Such an OS must be secure from all sorts of virus and other malicious software attacks.
- **Interface:** The digital wireless network must be universally usable, for instance, it must be usable by illiterates and must not require formal training for competent use. The interface should include basic functionality such as voice and speech, image and video messaging, and streaming VoIP.
- **Location Management:** To attract more mobile users especially in public areas, basic services that personalize user's experience need to be provided. The same can be achieved by integrating sensors and RF identification tags.

Deliverables:

The Cyber Security Research Centre will carry out studies and hosts seminars that move society towards rational and informed discussion of these critical changes. Center's mission is to encourage, promote, facilitate, and execute interdisciplinary research in areas related to the nexus of society and

the Internet. Future computer and communications networks will be more robust, more powerful and secure and more flexible under a wide variety of operating environments. The research work to be undertaken in the Centre and data collected here shall be of great benefit to the entire Research community who shall be perusing the similar area. We aim at creating a technology rich environment conducive to constructive discussions and evolving thoughts which will lead to innovative ideas in unwiring and digitizing the world securely at affordable costs. Besides the centre will:

- Aid and advise organizations in security policy enforcements, conduct of security audits and incident handling
- Provide various IT organizations including Police department, consultancy for design of secure networks including deployment of Security administration software like intrusion detection, management software for security software and vulnerability checking, protection against port scanners, password crackers etc
- Disseminate research results through journal and conference publications, technical reports, and public domain software.
- Train the manpower in cyber security related skills needed by state departments including police, network users, IT professionals, and network security specialists. By taking the policy seriously and teaching all of the stakeholders about their role in maintaining it, they will embrace the policy as an integral part of their jobs.
- Facilitate research work for undergraduate and postgraduate students and researchers in the concerned areas.
- Create a digital knowledge library in the form of WEB/FTP server consisting of information in the above mentioned areas.
- Undertake projects with Government of India, NASSCOM & industries in collaboration with allied Engineering Departments.
- Conduct interdisciplinary training programs for faculty and students

PLAN OF ACTION

Setting up of the Centre

This Regional Cyber Security Research Centre will be established in the Punjab Engineering College in collaboration with Chandigarh Administration and NASSCOM. The technical consultancy will be provided by NASSCOM and the funding to the project will be by Department of Information Technology, Chandigarh Administration, which will be done through Society for Promotion of Information Technology, Chandigarh.

Statement of Task:

This project will involve a survey of the research effort in cyber security and trustworthiness to assess the current mix of topics, level of effort, division of labor, sources of funding, and quality; describe those research areas that merit federal funding, considering short-, medium-, and long-term emphases and taking third-generation capabilities as a starting point; and recommend the necessary level for federal funding in cyber security research. Contemporary explorations of cyber security issues by a variety of parties will be factored into this examination. Technologies and approaches conventionally associated with cyber security and trustworthiness will be examined to identify those areas most deserving of attention in the future. In addition, this project will also seek to identify and explore models and technologies not traditionally considered to be within cyber security and trustworthiness in an effort to generate ideas for revolutionary advances in cyber security. Structural alternatives for the oversight and allocation of funding (how to best allocate existing funds and how best to program new funds that may be made available) will be considered and the Board of Mentors will provide corresponding recommendations.

The Board of Mentors for RCSRC shall consist of the following members:

ADMINISTRATION

1. Mr Lalit Sharma, IAS, Adviser to Administrator, Chandigarh
2. Mr. S.K.Sandhu, IAS, Finance Secretary, Chandigarh

NASSCOM

1. Mr. Kiran Karnik, President, NASSCOM
2. Mr. N.K.Saravade, Director, Cyber Security, NASSCOM

IT INDUSTRY

1. Mr. Arun Seth, Chairman, BT Worldwide
2. Mr. Prem Chand, Tech Mahindra
3. Mr. Akhilesh Tuteja, TCS

ACADEMIA

1. Dr. Vijay Gupta, Director, PEC, Chandigarh
2. Dr. Bhaskaran Raman, A. Professor, CSE, IIT Kanpur
3. Dr. Sanjeev Sofat, Professor & Head, CSE, PEC

Director, Information Technology, Chandigarh Administration shall be the Member Secretary for this Board for RSCRC.

PLAN ENVISAGED FOR CAPACITY BUILDING

At the very onset the RSCRC would begin its setting up in terms of Capacity Building. We see the central aspect of "capacity building" as a shared effort among all those involved in the programme to develop collectively our capacity for conducting excellent research around the important set of questions that drive our programme. The Capacity Building will be categorized as follows:

1. INFRASTRUCTURAL RESOURCES

The Capacity Building in terms of Infrastructural Resources would be started immediately. The activities classified under the same are as follows:

- (a) Renovation of the Building: Identifying key architects and getting the site renovated to present state of the art environment suitable for conducive research. The 2000 Sq. feet of area identified in the Department of Computer Sciences & Engineering, PEC, Chandigarh is to be renovated. The Engineering Department, UT has been asked to initiate this activity in consultation with the Director IT and the Centre Coordinators
- (b) Purchase of hardware and software has been started by SPIC.

2. MANPOWER

The Capacity building in terms of Manpower will be accomplished through learning by doing.

(i) Training

- Training the manpower in existing technologies and new tools and strategies.
- The Training shall be disseminated at various levels which shall act as human resource for the conduct of the entire activities to be undertaken.

The profiles can be:

- (a) In-house Faculty and faculty of other Engineering Colleges
- (b) Defense Personnel
- (c) Research Associates & Project Associates recruited in the Centre
- (d) N/W & System Administrators of Chandigarh Administration
- (e) Chandigarh Police

Besides this, the Undergraduate and postgraduate students can also be induced in the Centre for carrying out Research & development activities. Besides other formal curricula they can be professionally trained so that they can constructively contribute in disseminating useful results.

(ii) Extension Services

Outreach, through collaborations that deploy our security technology and encourage knowledge transfer for both public and private benefits will be undertaken. Dissemination of information related to Cyber Security will be done aggressively to increase community awareness of security technology, challenges and solutions. Special Cyber Safety events shall be organized as a part of Extension Services to spread awareness.

RESEARCH

To provide thought leadership to the nation and to the world among academics, practitioners, and policymakers. Collaborative research shall follow up so that academic researchers work hand in hand with industry researchers. Key research projects be identified based upon the manpower developed after the conduct of training mentioned above. RCSRC research shall improve our ability to design secure computer and network systems and protect them from attacks, enables people and organizations to form secure trust relationships across networked computing devices, and improves our understanding of the social, economic, and policy barriers to the development and deployment of such technology. The Center shall engage a multidisciplinary team of researchers and faculty and educate students in the broad field of cyber security. The Center shall focus on research in key technologies related to preparation for and response to emergencies at national, state and local levels. The RCSRC shall leverage prior applied research from military and civilian applications to develop new technologies unique to emergency preparedness and response. The research shall be geared toward the needs of first responders, incident commanders, emergency management officials and medical personnel. Drawing on the strengths from Computer Science & Engineering & IT, and NASSCOM the Center shall be a valuable regional and national asset for the development of emergency readiness and response technology.

PROPOSED PROJECTS

The abstracts of proposed Research projects that will be initiated in RCSRC are mentioned below:

Project-I

Title: Self defensive approach towards P2P worms exploits

Peer-to-peer (P2P) overlay networks enjoy enormous and ever increasing popularity both in real-life deployment (e.g., Gnutella and KaZaA) and also in the research community. While security issues for P2P networks have received attention, the main focus remains on ensuring correct operations within a P2P network in the face of failures and malicious participants. Examples include

maintaining the internal structure of a P2P network and fair sharing of resources. The threats that a large scale P2P network deployment poses to Internet security have largely been ignored. P2P worms exploit common vulnerabilities in member hosts of a P2P network and spread topologically in the P2P network, a potentially more effective strategy than random scanning for locating victims. This project shall identify the danger posed by P2P worms and initiate the study of possible mitigation mechanisms. In particular, the project shall explore the feasibility of a self-defense infrastructure inside a P2P network, outline challenges, and evaluate how well this defense mechanism contains P2P worms, and reveal correlations between containment and the overlay topology of a P2P network. The project shall layout a number of design directions to improve the resilience of P2P networks to worm attacks.

Project-II

Title: Secure Wireless City

The establishment of wireless city plays an essential role on such various government projects around the world. The challenge of this item is to provide valuable suggestions, including networking, security, and administration considerations, for building the secure wireless city. To provide a technical survey, the integration of heterogeneous wireless networks technologies will be investigated in and around Chandigarh. Additionally, current status and future trend of security considerations on deploying large-scale wireless networks will be analyzed.

The following are tentatively identified as an area

- The survey and analysis of wireless cities.
- The threat model analysis of wireless city, conducted
- The authentication issues on WiFi and WiMAX
- WiFi-WiMAX, inter-networking seamless roaming
- Extended VPN of secure wireless city.
- Practical applications on secure wireless city.

Project-III

Title: Digital Image Forensics

It is probably fair to say that it is no longer true that seeing is believing. The ease with which digital media can and is being manipulated and altered is simply stunning. At least one consequence of this is that images and video recordings no longer hold the unique stature as a definitive recording of events. And, while the technology to alter digital media is developing at break-neck speeds, the technology to contend with the ramifications is lagging seriously behind. There is, therefore, a critical need to develop tools to detect tampering in digital media. To this end, we will develop statistical tools for detecting tampering in digital images.

Project-IV

Title: Security through analysis and measurement for wireless LANs

With the rise of Voice over wireless LAN (VoWLAN), any complete WiFi security solution must address denial of service attacks, such as kicking off other clients, consuming excessive bandwidth, or spoofing access points, to the detriment of legitimate clients. Even authorized clients may be able to sufficiently disrupt service quality to make the network ineffective for legitimate clients. Our approach will provide a new foundation for wireless network security, ability to dynamically measure, analyze and protect a WiFi network against existing and novel threats, including rogue clients and access points, with a focus on VoWLAN use cases. Our goal is to support thousands of APs and clients, quickly recognize most new attacks, and generate few false alarms.

Project-V

Title: New Methods of Spoof Detection in 802.11 Wireless Networking

The explosive growth of 802.11 networks has coincided with an increased presence of security threats to these networks. A large proportion of these threats are in the form of spoof attacks. Spoof attacks involve one device assuming the identity of another to perform malicious behavior. The available security tools to detect such behavior are quite limited. Current methods of

sequence number analysis simply detect gaps in the monotonic incrementing series of sequence numbers in transmitted frames. However, these methods result in large amounts of false positives on wireless networks which experience even small amounts of frame loss. The unpredictable nature of environmental effects on signal propagation and a lack of signal strength stability due to calibration drift in low-quality wireless networking cards present significant challenges to using signal strength to detect wireless spoofs. A new methodology can thus be developed that can perform better detection and give less false positive rates than the popular tool: Snort-wireless's MacSpooF.

Project VI

Title: Securing WLANs on top of 802.1x

The project shall explore the practical problem of secure decentralized authentication and access control in wireless networks— WLANs (802.11 & 802.16). Many organizations are interested in securing connection access to their wireless (and wired) networks but the problem of accommodating guests continues to impede real deployments. This project will transform a working prototype solving this problem into ready-to-use technology that can be added to an 802.1x authenticated network. This project shall also explore a deeper problem: if the trust flow expressed by an infrastructure's clever PKI does not match the trust flow the human organization requires, then the human users will find a way to achieve their goals that breaks the infrastructure. This project's approach marries the security of standard X.509 PKI tools with the flexibility of delegation.

As the implementation of the project progresses, more research projects will be added and also the scope of the existing ones will be enhanced.