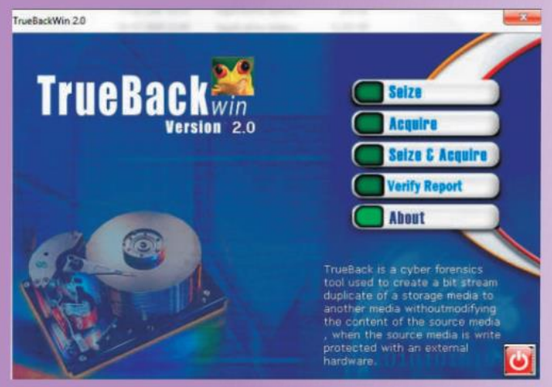
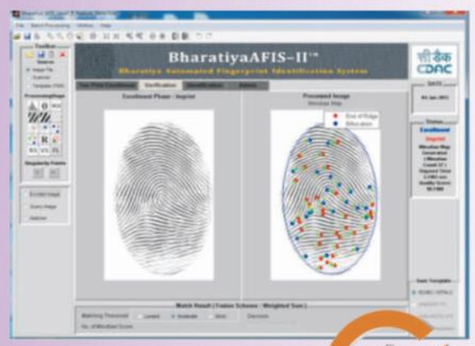
Services Offered

Empanelled by Indian Computer Emergency Response Team (ICERT), C-DAC offers various cyber security auditing services like

- Consultancy for ISMS auditing
- Cyber forensic analysis, training and laboratory development
- Malware analysis
- Vulnerability assessment and penetration testing of web applications and networks





Courses Offered in Cyber Security

C-DAC offers short term courses on topics such as Database security, Ethical hacking, Perimeter security, Security engineering, Web application security, Wireless security, Security administration Linux, Cyber forensics, Cyber crime, IT law, Mobile security, etc.

OEM of SRIT

Cyber Security

- Biometrics
- Cyber Forensics
- End Point Security
- Network Security
- SCADA Security
- Cloud Security
- Honeynet Technologies
- Mobile and Web Security

SRIT

Increased penetration of the Internet has led to the increase in cyber attacks on Information Technology (IT) infrastructure. Cyber attacks on smartphones are also growing due to the increasing growth of 3G Internet services and business transactions using mobile phones. In order to make the IT infrastructure and online business transactions resilient against these attacks, there is a need for cutting-edge Research and Development (R&D) in cyber security. C-DAC has been pursuing R&D in a number of sub-areas in cyber security domain.

Areas of Activities

Biometrics

In the field of biometrics, C-DAC focuses on developing technologies for fingerprint, iris, vascular, periocular, handwritten signature as well as voice and face recognition. Research efforts are also being made for developing multi-biometric products/solutions (using fingerprint, iris, etc. modalities).

Cyber Forensics

C-DAC developed indigenous tools for collecting digital evidence pertinent to different areas like disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

End Point Security

C-DAC has developed solutions to provide defence mechanism to the end point security threats. These solutions span across mitigating threats through USB mass storage devices, data exfiltration, malicious/ unknown applications, application behaviour, malware and the web browser. Behaviour heuristics as well as applications behaviour whitelisting approaches are used and various solutions are developed. Solutions are being developed to address malware threats through browsers on desktops and mobiles.

Network Security

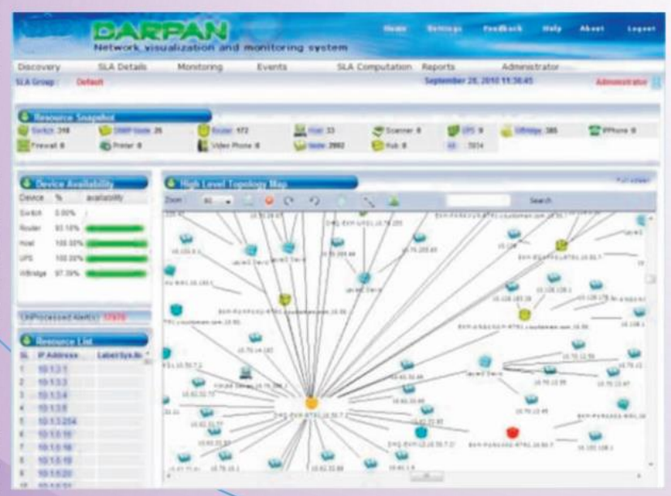
C-DAC is focusing on adaptive intrusion detection, dynamic firewall, unified threat management and network management using behaviour based model. These approaches enable the detection engines to learn new attack patterns by continuously analyzing various events, such as, network traffic, host parameter, logs, etc.

Mobile and Web Security

C-DAC is developing mobile device security solutions to provide features like secure storage, application monitoring and control, local and remote secure device backup and restore, remote erase/ lock, and call and SMS blacklisting/whitelisting, etc. This solution also supports offline application analyzer and kernel level enforcer. C-DAC is developing an automated Web Security Assessment Framework, to assess the vulnerabilities and risk in a network environment.

SCADA Security

Since SCADA systems are getting integrated into the Internet, this poses new kinds of threats to the critical infrastructures. C-DAC is building counter-measures against SCADA system vulnerabilities and threats.



Cloud Security

C-DAC is developing solutions to minimize the security risks associated with using cloud computing and storage services for achieving privacy, integrity and availability with elastic load balancing. The current focus is to develop solutions for access control mechanisms, data encryption and Distributed Denial-of-Service (DDoS) attack detection mechanisms.

Honeynet Technologies

C-DAC has designed a distributed honeynet system, which is a collection of honeynets distributed over the Internet or any other large network. These honeynets send data to a central analysis point. This setup can play a critical intelligence-gathering role for network defenders.

Solutions

Biometric Solutions

- **The Bharatiya AFIS Suite:** Bharatiya Automated Fingerprint Identification System Suite is a family of fingerprint biometric products (Systems and SDKs), complying to the various International Standards
- **Bharatiya-IRIS:** Iris Recognition and Identity Solution for identification of individuals using their irides
- **Touch screen-based Bharatiya Biometric Attendance System:** Centralized, web-based, biometric attendance system (using iris or fingerprint for marking the attendance)
- **Automatic Face Recognition System:** It can identify a person from his/her facial image and supports one-to-many searching

Cyber Forensic Solutions

- **Disk Forensics Tools:** Software suite comprising of disk imaging (True Imager), data recovery and analysis (Cyber Check), software for tracing the sender of an e-mail, Forensic Data Carving (F-DaC), Forensic Registry analysis (F-Ran) and Forensic Thumbnail extraction (F-Tex) tools
- **Network Forensics Tools:** Software suite comprising of Network Session Analyser (NeSA), Forensic Log Analyzer and software for tracing the sender of an e-mail
- **Mobile Device Forensics Tools:** Software solution for acquisition and analysis of mobile phones, smart phones, Personal Digital Assistants (PDA) and other mobile devices (Mobile Check), software for analyzing Call Data Records of various service providers (Advik) and forensic solution for imaging and analyzing SIM cards (SIMXtractor)
- **Live Forensics Tool (Win Lift):** Software solution for acquisition and analysis of volatile data present in running Windows systems
- **TrueTraveller:** Portable Forensics Toolkit

End Point and Network Security Solutions

- **Application and Device Control (ADC):** Centralized solution for application and device control
- **AppSamvid:** Application whitelisting solution for the desktops
- **USB Pratirodh:** USB mass storage device control software targeted towards securing end systems from unauthorized usage of portable USB storage devices
- **DARPAN:** Network management solution
- **Guard Your Network:** Network intrusion detection and prevention appliance
- **EDGE:** LAN and WAN monitoring solution
- **CHAKRA:** Dynamic firewall solution with capabilities to create rules automatically

Mobile and Web Security Solutions

- **m-Safe:** Mobile SDK for secure communication and storage
- **WebSAFE:** Web application Security Assessment FramEwork- Automated web based tool to perform security assessment of web applications and report the risk associated with the identified vulnerabilities along with generic counter-measures
- **JSGuard:** Browser add-on to detect and defend from malicious URL
- **PHP Application Vulnerability Scanner (PAVS):** Source code scanner for finding the code vulnerabilities in PHP based web applications