Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

Be aware of
Password Threats

InfoSec Concept : 4

For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Hyderabad Campus, Kukatpally, Hyderabad - 500 085.
Tel: 040-2315 0115. Fax: 040-2315 0117. E-mail: *isea@cdac.in*

InfoSec Magazine 2013-Edition-I

Credits

Editorial Committee

Shri.Sanjay Kumar Vyas
Joint Director, DeitY

V.Muralidharan,Director
Mr.Ch.A S Murty &
Mrs.Indraveni K
Shri G.V.Raghunathan,
Consultant
C-DAC Hyderabad

Design Team
K.IndraKeerthi
S.Om Aarathi

Action Group Members

Dr.Kamlesh Bajaj
Data Security Council of India
Dr.Dhiren R Patel
Professor of Computer Engineering,
NIT Surat
Shri.Sitaram Chamarthy
Principal Consultant, TCS
Dr.N. Sarat Chandra Babu
Executive Director,
C-DAC Bangalore
&
HOD, HRD Division
DeitY, Government of India

Acknowledgement

HRD Division
Department of Electronics
& Information Technology
Ministry of Communications
and Information Technology
Government of India

Comments & Feedback
mail us to
isea@cdac.in

InfoSec Quiz

It is one of the malware
(a)gossips (b)threat (c)vulnerability (d)ransomware

We can click on the links received from known or unknown emails ID's
(a)True (b)False

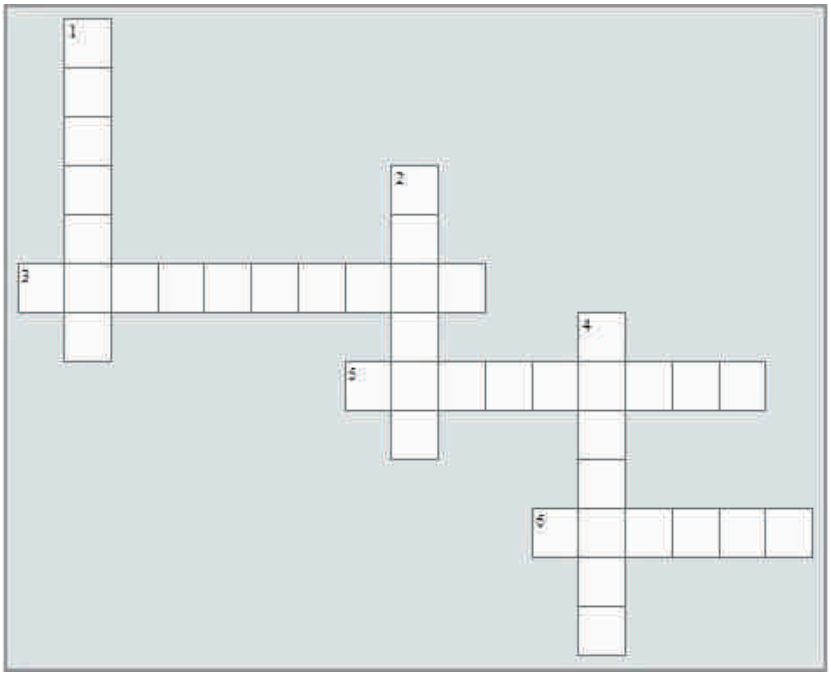
We can copy the content available over internet and we cannot be sued for copyright violations
(a)True (b)False

A Hacked computer can be used to
(a)Infect other systems (b)Harm your system by malware
(c)Help your system with latest updates (d)Both a and b

My email is private and no one can look into it
(a)True (b)False

logon to
www.infosecawareness.in
to participate in Infosec Contest and win prizes

InfoSec Crossword



Across:

3. uses an algorithm that transforms information and making it unreadable & inaccessible to anyone except for those who have the appropriate credentials
5. restrict network activity to known applications, and prevent malicious people and programs from exploiting holes in operating systems and other software applications
6. ensures that the information you need is there when you need it and it can recovered if the information is damaged in the system.

Down:

1. It is one of the methods of social engineering
2. The information stored on client computer by a webserver is called a
4. is harmful software, usually installed without your knowledge

InfoSec Guess Tip

Guess the Tip which best suits the cartoon by logging in to *http://www.infosecawareness.in*

InfoSec Cartoon

Ensure that your transaction is ended/completed at ATM machine before leaving.

InfoSec Tip

All Wi-Fi equipment support some form of encryption,so enable them.

Wi-Fi Security

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Tips for securing Wireless Communications

- **Always use strong password for encryption**
  A strong password should have atleast 15 characters, uppercase letters, lowercase letters, numbers and symbol. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key. Do not use WEP for encryption, rather use WPA/WPA2.
- **Restrict access to the Access Point based on MAC address**
  In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
- **Change the default username and Password of the Access Point**
  Most of the users do not change the default passwords while configuring the Access Point. But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
- **Do not broadcast your network name**
  SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- **Disable DHCP service**
  When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.
- **Shutdown the Access Point when not in use**
  Hackers try to brute force the password to break the keys, so it is good practice to turnoff the Access points during extended periods of Non-use. For more details visit

For more details visit
www.infosecawareness.in

Password Threats

Various Techniques used by hackers to retrieve Passwords

Bruteforce Attack

Another way of stealing the password is through guess. Hackers try all the possible combinations with the help of personal information of an individual. They will try with the persons name, pet name (nick name), numbers (date of birth, phone numbers), school name...etc. When there are large number of combinations of passwords the hackers uses fast processors and some software tools to crack the password. This method of cracking password is known as "Brute force attack".

Dictionary Attack

Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

Never use dictionary words (like animal, plants, birds or meanings) while creating the passwords for login accounts.

What is Password?

Password is a key or a Secret word or a string of characters which is used to protect your information from bad people in the cyber world. It is used for authentication, to prove your identity or to gain access to resources. It should be kept secret from access of unauthorized users.

Why Strong Password?

Keeping a strong password may not be sufficient as if your answers in the secret question section of your online profile are easy to find, a bad guy/ hacker may be able to convince the web mail service password recovery mechanism to handover the password to attacker/hacker

Shoulder Surfing

One way of stealing the password is standing behind an individual and over look their password while they are typing it (Shoulder Surfing) .Shoulder Surfing is a direct observation technique, such as looking over someone's shoulder, to get passwords, PINs, other sensitive personal information and even listen in on your conversation if you give your credit-card number over the phone.

Shoulder surfing is easily done in crowded places. It's comparatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. It can also be done long distance with the help of binoculars or other vision-enhancing devices. Your confidential information will be at risk if your passwords are observed by Shoulder Surfers. They can use your password information for logging into your account and they may do harm to your information.

How to prevent it?

- Be aware of Shoulder Surfers at public places or schools while you are entering your passwords into the login accounts.
- Do not reveal your passwords in front of others or type your usernames and passwords before the unauthorized persons.
- Cover the keyboard with paper or hand or something else from viewed by unauthorized users.

Your password should contain

Uppercase letters : A-Z
Lowercase letters : a-z
Numbers : 0-9
*Special characters : $@!&^**

InfoSec Concept

Never talk about your password in front of others

the access to your information. The operating system does not know who is logging into the system, it will just allow any person who enters the credential information into the login page. The persons like strangers after getting access to your information they can do any thing.

Sending your password information through network

The Hackers even get the password information by Sniffing the network traffic which is travelling on the network or even can get the password information by listening to your phone call conversation with others

Never send sensitive details like password or credit/debit numbers through e-mails.

Sharing your passwords with strangers

Sharing the passwords with the unknown persons (strangers) may also lead to loss of your personal information. They can use your login information and can get

For more details visit www.infosecawareness.in

Guidelines for maintaining a good password

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Do not use the name of things located around you as passwords for your account.

Possible Vulnerabilities

- The passwords could be shared with other persons and might be misused.
- The passwords can be forgotten.
- The Stolen passwords can be used by unauthorized user and may collect your personal information.

Do not use same password that was used earlier.

Never write your passwords on paper (or) anywhere else for referring

Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

सी डैक
CDAC

We always use
strong & easy to remember
PASSWORD[S]
for Internet applications
Do You ?

for more details visit

www.infosecawareness.in

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Hyderabad Campus, Kukatpally, Hyderabad - 500 085.
Tel: 040-2315 0115. Fax: 040-2315 0117. Website: www.cdachyd.in esuraksha@cdac.in

USB Pratirodh

Regulating removable storage device access

In the world of information age, the data stored in the computer is most valuable assets to any organization. It may include pricing details, trade secrets, Intellectual property, customer list, business plans and even personal information. These are the assets that enable a company to distinguish itself from the competitors. Due to this, a security breach is easy to occur at any time, like anyone can use a mass storage device and copy these valuable assets. And if it happened, the effect will be disastrous and irreversible. Moreover USB mass storages become the main propagator of all malicious software. The crux is that controlling or blocking the usage of USB mass storage device is vital to any organization no matter what data they handle.

CDAC Hyderabad has come up with a solution, for securing from the threat of USB removable media, called USB Pratirodh. USB Pratirodh is a software solution which controls unauthorized usage of portable USB storage devices. The USB Pratirodh blocks and controls the usage of removable storage media like pen drive, external hard drives, cell phones, IPods, camera and any USB mass storage devices. Only authenticated users can access the removable storage media.

" Your computer stores information, information is knowledge, Knowledge is the power, so it should be protected "

Features

Device Control:

All USB devices are uniquely identified. User can add or remove the devices into the data base. User can bind one or more USB Devices to be accessed using enabled username. If it is a new device user will be notified and should provide user name, password, and description to add the data to the data base.

User authentication:

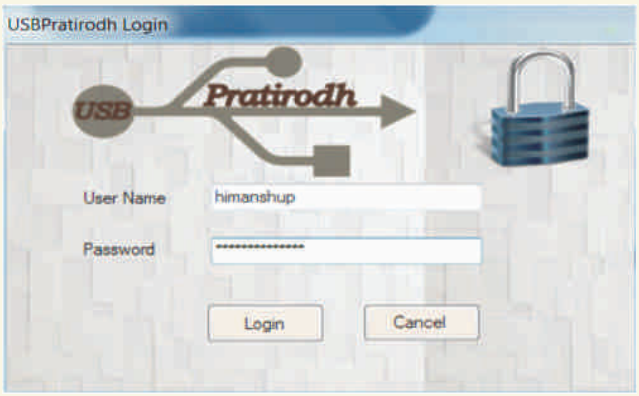
Whenever a pen drive got plugged in user will be asked to authenticate with user name and password. Only authenticated user can access the device. If the user fails to authenticate and try to access the device, user gets a access denied message

Co-existence:

USB Pratirodh is designed in such a way that it blocks only USB mass storage devices. It can co exist with other USB devices like mouse, keyboard, webcam, etc. User does not get any notification or disturbance on using other USB devices other than Mass storage devices. USB Pratirodh co-exists with other security solutions.

Support for both Windows and Linux:

USB Pratirodh runs Windows as well as Linux environment. It support Windows XP SP2, Vi s ta, Windows 7 and Linux (Ubuntu , BOSS and SUSE, etc)



Benefits

- USB device control with password protection
- Data Encryption on USB devices
- Auto run protection and Malware Detection
- Configurable read/write privilege protection

For more details visit:
http://cdachyd.in/products/usb-pratirodh

Wireshark

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.

Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

Wireshark Online Tools

Editor Modeline Generator

Suppose you have some code which may be editied by people with different text editors and coding style preferences. As discussed by Jamie Zawinski, indentation width, tab width, and indentation behavior can vary widely and can often be a religious (and in the case of Python, sanity) issue.

Some editors are nice enough to let you configure indentation and tab behavior inside the file you're editing. This feature has many different names, such as "modelines," "buffer-local properties", or "file variables". We use the term "modline" here.

The form below lets you create modeline blurbs that you can copy and paste into the file you're editing. Simply select the settings you would like to apply, then copy and paste. You can also create modelines from a set of existing coding styles below.

IPv4 and IPv6 Connectivity Test

What is this?
It's a web page that tries to test your IPv4 and IPv6 connectivity.

What does it do?
It tries to load images from an IPv4-only version of the site (ipv4.wireshark.org) and an IPv6-only version of the site (ipv6.wireshark.org) and updates the web page to indicate success or failure.

Why do I see funny block characters?
We draw a Unicode HEAVY CHECK MARK (U+2714) to indicate success and a HEAVY BALLOT X (U+2718) to indicate failure. Some browsers or operating systems may not be able to display those characters, particularly older ones. If this is the case for you you might try installing DejaVu.

OUI Lookup Tool

The Wireshark OUI lookup tool provides an easy way to look up OUIs and other MAC address prefixes. It uses the Wireshark manufacturer database, which is a list of OUIs and MAC addresses compiled from a number of sources.

Directions:
Type or paste in a list of OUIs, MAC addresses, or descriptions below. OUIs and MAC addresses may be colon-, hyphen-, or period-separated.

String-Matching Capture Filter Generator

What is this?
It's a web page that lets you create capture filters that match strings in TCP payloads.

What does it do?
It takes the string you enter, splits it into 1, 2, or 4 byte chunks, converts them to numbers, and creates a capture filter that matches those numbers at the offset you provide.

It should handle most UTF-8 characters but this hasn't been tested.

What is it good for?
You can use it to filter things like top-level HTTP requests ("GET / HTTP/1."), HTTP responses ("HTTP/1."), POP3 logins ("USER"), and lots of other things.

What is it NOT good for?
Matching strings at arbitrary locations. You can't do that with capture filters (BPF doesn't support it) You need to use the "matches" or "contains" display filter operators instead. You'll have to use the "matches" display filter operator for case insensitive matching as well.
What's up with all of the fancy bit-twiddling in the TCP header?

It makes sure we skip over any TCP options that might be present. See Sake's explanation for more details.

WPA PSK (Raw Key) Generator

The Wireshark WPA Pre-shared Key Generator provides an easy way to convert a WPA passphrase and SSID to the 256-bit pre-shared ("raw") key used for key derivation.

Directions:
Type or paste in your WPA passphrase and SSID below. Wait a while. The PSK will be calculated by your browser. Javascript isn't known for its blistering crypto speed. None of this information will be sent over the network.

For Wireshark blog visit
https://blog.wireshark.org/

For Wireshark online tools visit
http://www.wireshark.org/tools/

Features

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

For more details visit
http://www.wireshark.org/about.html

Win32/NetTraveler.b

It has been observed that new variants of malware family Win32/NetTraveler is spreading widely. It spreads via spear phishing emails containing attached malicious Microsoft office document. This malware uses malicious netTraveler toolkit (data exfiltration tool). This malware uses compression techniques to safely transfer stoslen data to Commant and Control.

The malware performs the following function:

- Reporting a new infection to its author
- Receiving configuration or other data (ex .cfg, .cfn)
- Downloading and executing arbitrary files related to updates and other malware
- Receiving instruction and commands from remote attacker
- Upload stolen data of victim machines (e.g .doc, .xls, .ppt, .pdf, .cdr etc)
- Capture keystrokes

Countermeasures

- Perform scanning on computer for possible infection with the removal tools mentioned below
- Monitor traffic for the above mentioned domains at premier level and block the same and also identify the infected computer system and clean the same
- Exercise caution while visiting links within emails received from untrusted users or unexpectedly received from trusted users
- Do not download and open attachments in emails received from untrusted users or unexpectedly received from trusted users.
- Exercise caution while using external drives, disable autoplay
- Autorun should be disabled e.g consider using antimalware solution like Panda USB vaccine to thwart Autorun malware
- Exercise caution while visiting links to web pages
- Protect yourself against social engineering attacks.
- Do not visit untrusted websites
- Enable firewall at desktop and gateway level and disable ports which are not in use
- Use genuine operating system and application software only. Avoid downloading genuine or pirated software from untrusted sources
- Keep up-to-date patches and fixes on the operating system and application software
- Use Microsoft's Enhanced Mitigation experience Toolkit (EMET) to mitigate risk
- Use Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources
- Keep up-to-date antivirus and antispyware signatures at desktop and gateway level
- Selectively disable Java/Flash, javascript (Internet Explorer)

Win32/Beebone

It has been observed that new variants of Trojan win32/Beebone are spreading widely. This is a Trojan downloader family which silently downloads and installs other malware programs without user consent

This Trojan contacts the following remote hosts:

[Replace "[d0t] " with "." For actual URL]

- Domain[d0t]dns00[d0t]net using port 8080
- 38071[d0t]dns6y[d0t]com and 10361[d0t]dnshy[d0t]eu using port 443
- 14121[d0t]dns6y[d0t]net, 61300[d0t]dns6y[d0t]net, 37479[d0t]dns6y[d0t]net, 32891[d0t]com,51321[d0t]z0dns[d0t]com, 98500[d0t]0xdns[d0t]net using port 2323

Malware contacts to the above mentioned domains for the following purposes

- To report a new infection
- To receive configuration or other data
- To download and execute arbitrary files
- To receive instructions from a remote attacker and
- To upload the data taken from the affected computer

Countermeasures:

- Exercise caution while using external/removal storage devices
- Disable Autorun functionality in Windows
- Disable AutoPlay functionality in Windows
- Keep up-to-date patches and fixes on the operating system and application software
- Do not visit untrusted websites
- Keep up-to date Antivirus & Antispyware signatures at desktop & gateway level
- Use strong passwords & also enable password policies
- Protect yourself against social engineering attacks
- Enable firewall at desktop & gateway level and disable ports that are not required
- Use limited privilege user on the computer
- Exercise caution while opening attachments and accepting file transfers via instant messaging services.
- Exercise caution while visiting links to webpages
- Exercise caution while opening email attachments received from intrusted sources or received unexpectedly from trusted sources.
- Avoid downloading pirated software

For more details visit
www.cert-in.org.in

THE TIMES OF INDIA | Tech News

Home City India World Business Tech Sports Entertainment Life & Style Women Spirituality NRI

Ransomware virus threat getting worse warns McAfee

PTI Nov 25, 2013, 04.54PM IST

Tags: Ransomware | McAfee | Malware | Growing malware threats | android

NEW DELHI: Taking advantage of anonymous payment services, cyber criminals are increasingly using a malicious software 'ransomware' that holds a computer hostage until the victim pays to free it, online security firm McAfee says.

http://articles.timesofindia.indiatimes.com/2013-11-25/internet/44449001_1_malware-ransomware-mcafee-labs

DECCAN Chronicle

Tuesday, Dec 03, 2013 | Last Update : 05:48 PM IST

TRENDING TOPICS:

NEWS STATES INTERVIEWS ENTERTAINMENT SPORTS LIFESTYLE COMMENTARY GALLERIES ASTROGUIDE MA

Home » News » Current Affairs

Nigerians still 'win' lottery fraud

DC | 27th Nov 2013

Hyderabad: Two Nigerians who were caught by the Mahankali police bought expensive handicraft goods in bulk and exported them to Nigeria with the money they had earned through fraud.

The duo — Patrick Okwuokenye, 31, and P. Festus Iteh, 28, both from Gbor city of Nigeria — were living in Delhi and luring innocent people after convincing them that they had won lottery worth crores of rupees.

"They would ask the victim to deposit the processing charges in different bank accounts and withdrew the money through ATMs in Delhi. They used bank accounts of Indian citizens for the money transactions to evade police,"

http://www.deccanchronicle.com/131127/news-current-affairs/article/nigerians-still%E2%80%98win%E2%80%99-lottery-fraud

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

Supported by

Department of Electronics & Information Technology
Government of India

Executed by

www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Hyderabad Campus, Kukatpally, Hyderabad - 500 085.
Tel: 040-2315 0115. Fax: 040-2315 0117. E-mail: *isea@cdac.in*