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

InfoSec Newsletter

March - April 2016

InfoSec Concept 4

Wi- Fi Security

InfoSec
Tools
Alerts
News
Workshop

Participate in InfoSec
Quiz
Crossword
Guess the tip

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
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via
Keshavagiri (Post) Hyderabad - 500005, Telangana

InfoSec Newsletter

March - April 2016

Credits

Prof. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
I L Narasimha Rao
K Indra Veni
K Indra Keerthi
P.S.S.Bharadwaj

Action Group Members
HOD (HRD), DeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, DietY

Compiled by
G V Raghunadhan
Ch A S Murty

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Department of Electronics &
Information Technology
Ministry of Communications &
Information Technology

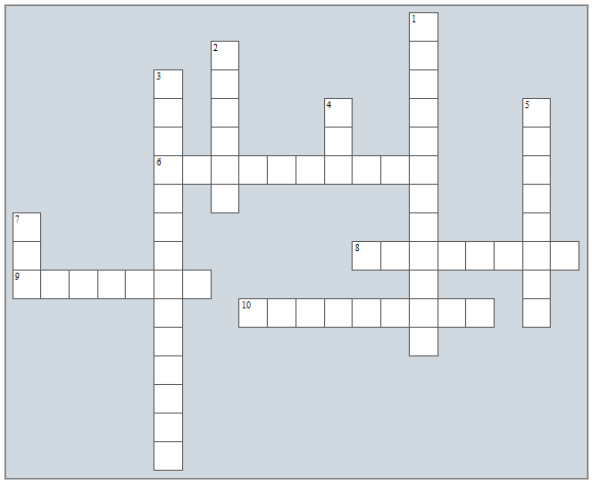
For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

InfoSec QUIZ

1. Laws granting legal right to the creator of a work, which require others to gain permission before using that work?
   A) Patentright B) Copyright
2. A person who harasses, taunts, or teases online?
   A) Cyberbully B) Hacker
3. Technology that prevents users from visiting inappropriate websites?
   A) Firewall B) Web filtering technology
4. A computer program designed to damage computer files. It replicates itself?
   A) Trojan B) Worm
5. Advertising supported software that automatically plays or displays ads?
   A) Adware B) Spyware

InfoSec CROSSWORD



Logon to
www.InfoSecawareness.in/contest
to participate in InfoSec Contest and win Prizes

Across

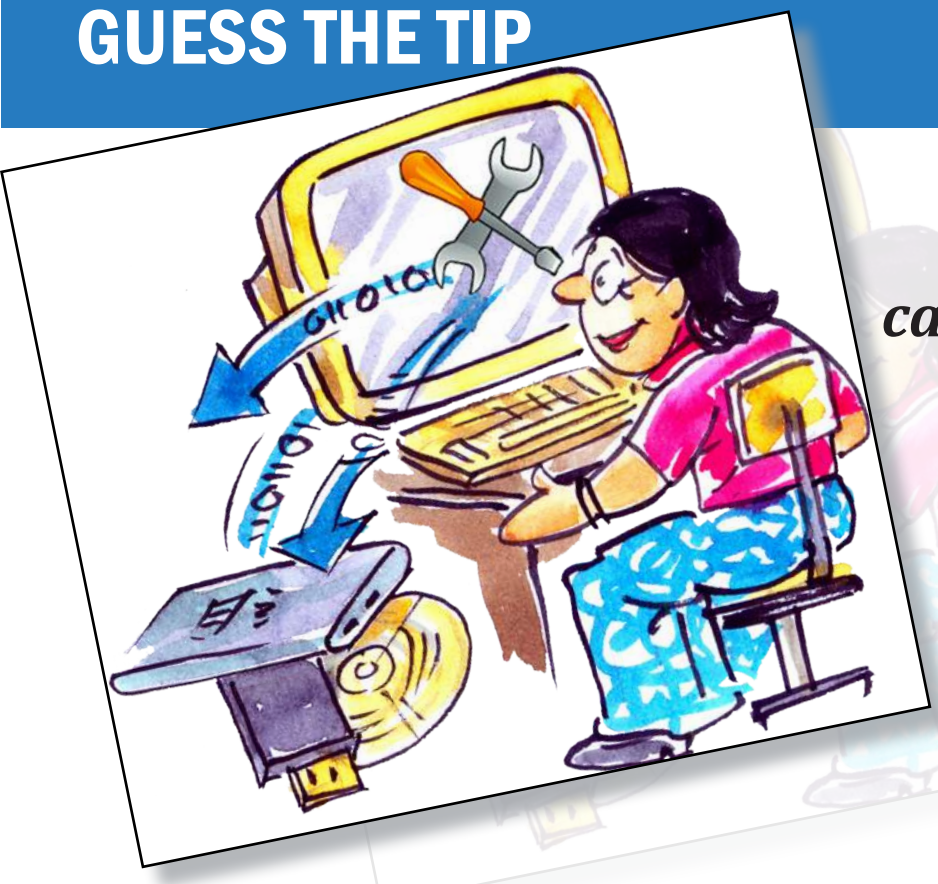
6. is the most effective way to achieve data security
8. converting enciphered text to plain text by means of a cryptographic system
9. is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express them selectively
10. A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer

Down

1. is the validity and conformance of the original information.
2. The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information
3. ensures that resources are only granted to those users who are entitled to them
4. A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator
5. communication is the transfer of information between two or more points that are not connected by an electrical conductor
7. is a simple, high-speed encryption technique built into 802.11 WLANs, using 40-bit keys

**** Answers will be announced in the next newsletter***

InfoSec GUESS THE TIP



Guess the Tip which best suits the cartoon by logging in to

www.InfoSec awareness.in

InfoSec TIP

You are responsible for safeguarding your user ID and password. Never write your passwords on paper (or) anywhere else for referring

About Passwords

Password is a key or a Secret word or a string of characters which is used to protect your digital assets or information from others in the cyber world. It is used for authentication, to prove your identity or to gain access to your own resources. It should be kept secret to prevent access by unauthorized users. In social networking sites like Facebook, Orkut, and LinkedIn each of which is studded with answers to commonly used security questions such as favourite place, school, college, etc.. Avoid using them as passwords.

Importance of Passwords

- User ID represents the identity of an individual, while a password helps to validate it.
- A password helps individuals in protecting personal information from being viewed by unauthorized users. Hence it is important to secure passwords.

Possible Vulnerabilities with Password

- Passwords shared with other persons might be misused.
- Passwords can be forgotten
- Stolen password can be used by unauthorized user who may collect your personal information
- Easy Passwords such as with name, date of birth, mobile numbers could be guessed by anybody and misuse them
- If you use same password for all accounts, It would be easy for the hackers to crack all account passwords

For more details visit : www.infosecawareness.in

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 the security levels to be set on these devices, these get vulnerable. By taking advantage of these unsecured Wi-Fi devices, terrorists and hackers fulfill their needs.

Wi-fi Security

Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points(wireless routers).Anyone in the range of those Access points can connect to any of these Access Points if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victims computer to get control on it through Internet, etc.

All these criminal acts will naturally be associated with the legal user of Access Point(wireless router). It is up to the legal user of the Access Point to defend himself to prove that he has not been involved in these acts. It is the responsibility of the user to secure his/her own Access Point.

Never auto-connect to open Wi-Fi networks in public places

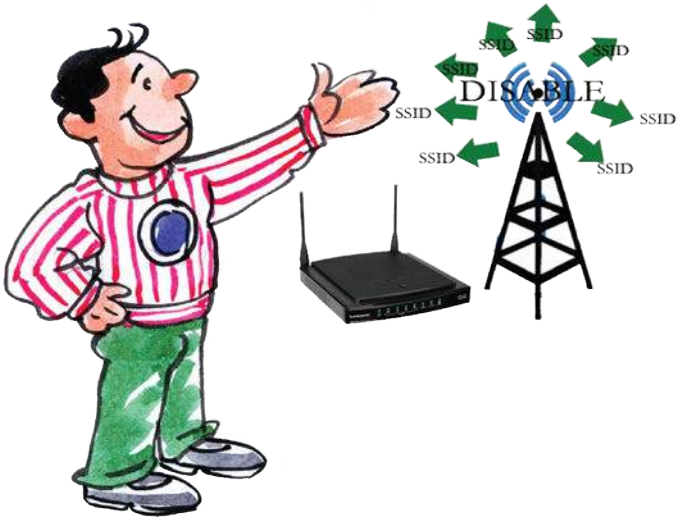
Lets see some real incidents that took place in the recent years.

- Terrorists and hackers used unsecured Access Points to perform illegal activities on the Internet.
- Hackers penetrated into open Wi-Fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private emails sent by the guests. The hackers then attempt to extort money from the hotel chain by threatening to publish the emails.(www.crpcc.in)
- Just 5 minutes before Delhi blasts on September 2008 terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai to send terror emails to authorities and news channels. These hackers do not leave a trail of footprints for the investigators to arrive at a logical conclusion. The audit trail ends at Wi-Fi Access Point of the legal user. So it is imperative for the users to secure their own Access Points(wireless router).

The following are the steps to secure an Access point

Disable SSID broadcasting in wireless access point

Secure your wireless communication with additional network security such as SSH, or VPN, or SSL tunneling and turn off the wireless devices when not in use



Turn off wireless networks when not in use

Types of Attacks on Wireless Environment

- **Denial of Service Attack**
  Denial of Service Attack aims at preventing the users from accessing the network resources. In a Wireless network, denial of service attack can be applied in various ways.

- **Man-In-Middle Attack in Wifi Devices**
  Performing Man-In-Middle Attack in a wireless network is much easier, when compared to wired network. As the transmissons from an accesspoint is broadcasted, it is easy for an unauthorised user to collect the traffic sent by other wireless clients. And the process of collecting the packets in this manner is known as Eavesdropping. Also the third party user can manipulate the packets sent to the legitimate users which results in breaking the users privacy.
  So In order to avoid these kind of attacks, Strong encryption should be used for transmitting the data between wireless client and accesspoint.
- **WarDriving**
  It is a process of tracking Wi-Fi hotspots located at a particular place, while moving with a hand held device or a laptop in a vehicle. This helps the user in finding out the accesspoints that doesnot use encryption and takes control over it for performing the attacks on the network

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. It is more secured.

- **Always use the maximum key size supported by accesspoint for encryption**
  If the keysize is large enough, then it takes more time to crack the key by the hacker. Also it is recommneded to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.

Be careful at public Wi-Fi hotspots

- ***Turn Off Sharing***
- ***Enable Your Firewall***
- ***Use HTTPS and SSL Whenever Possible***
- ***Consider Using a Virtual Private Network***
- ***Turn Wi-Fi Off When You Aren't Using It***

- **Isolate the wireless network from wired network with a firewall and a antivirus gateway.**
  Do not connect the accesspoint directly to the wired network. As there is a chance of compromised wireless client inturn effecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the accespoint and the wired network.

- **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.

- **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 turn off the access points during extended periods of Non-use

Change your default administrator passwords and usernames for your Wi-Fi devices

- **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.

- **Always maintain a updated firmware**
  Updating the firmware of accesspoint is recommended, as it will reduce the number of security loop holes in the accesspoint.

- **Use VPN or IPSEC for protecting communication**
  When the information flowing from wireless client to the wired network receiver is critical, then it is recommended to use VPN or IPSEC based communication so that the information is protected from sniffers in the network.

- **Disable DHCP service**
  When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. With enabled DHCP service attackers can easily to connect to the network once they get associated with the Access Point

How the attack occurs in Wifi Environment ?

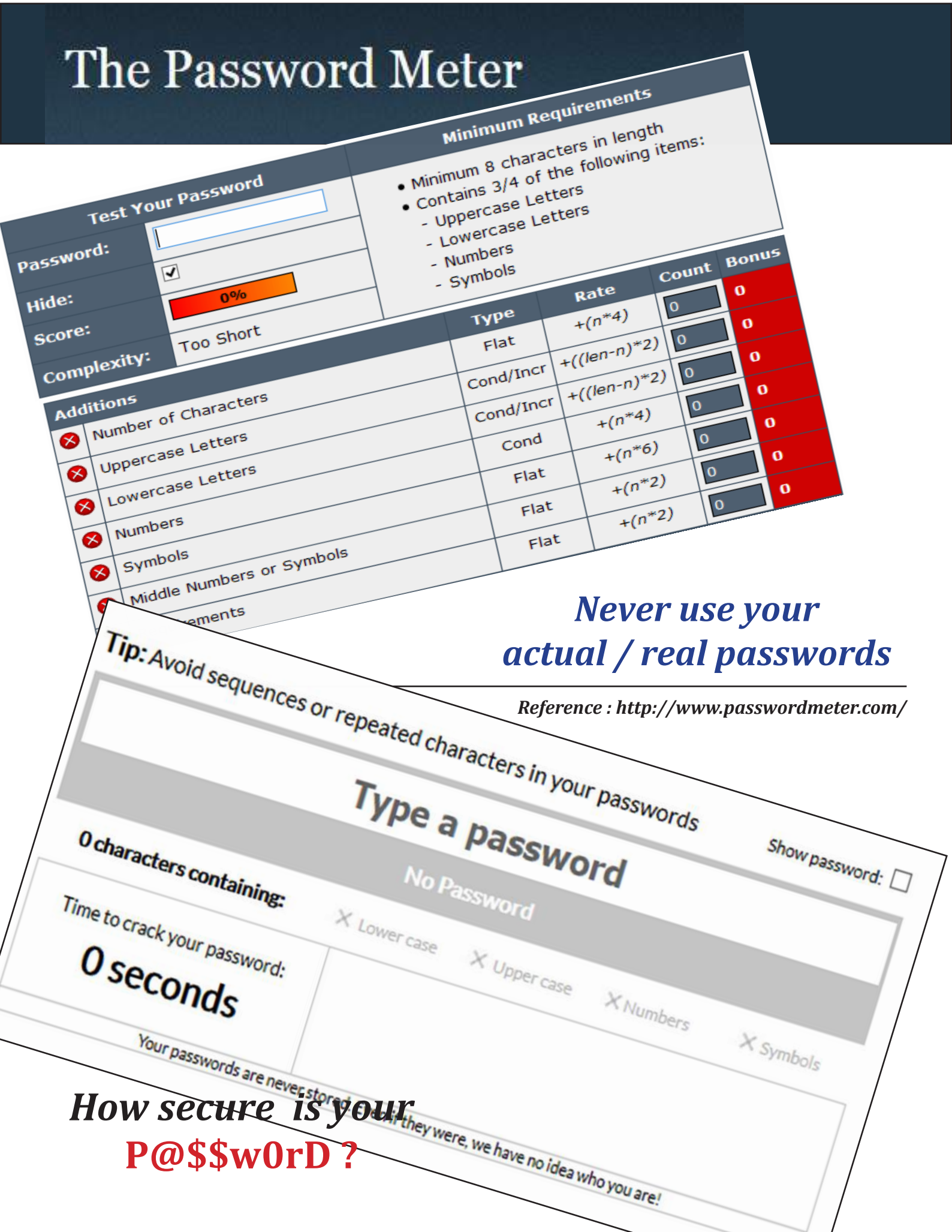
- At the physical layer of TCP/IP Model, denial of service attack can be implemented by introducing a device which will generate noise in the same frequency band in which wireless accesspoint is operating. This makes the users who are trying to connect to the accesspoint may not be able to connect to it.
- Also the other possibility of Denial of service Attack is spoofing the accesspoint.Normally wireless clients connect to the wired network with the help of an accespoint. For associating with the accesspoint they require SSID of it. When an unauthorised user places an accesspoint with the same SSID, then there is a chance of authorised user getting associated with the attackers accesspoint. If that happens, the attacker will try to collect sufficient number of packets from the wireless client and cracks the WEP key used by the legitimate accesspoint. Then the attacker gets associated with the legitimate accesspoint and generates large ping requests in the network or generate some abnormal traffic, which may finally result in Denial of Service Attack.

Posters and stickers released by
Shri K. Shankar, IPS, Additional Commissioner of Police, Chennai in the presence of Prof. N Balakrishnan IISc, Bangalore and Prof. V Kamakoti, IIT, Madras

Posters and stickers released by
Smt. G.Subbulakshmi, Superintend of Police (SP) Salem, Tamil Nadu in the presence of
Shri E. Magesh, Director, C-DAC, Hyderabad

InfoSec TOOLS :

Check your password strength



Never use your actual / real passwords

Reference : http://www.passwordmeter.com/

How secure is your

P@$$w0rD ?

Common mistakes and misconceptions

- Replacing letters with digits and symbols. This technique is well known to hackers so swapping an "E" for a "3" or a "5" for a "$" doesn't make you much more secure
- That meeting the minimum requirements for a password makes it strong. By today's standards, an 8-character password won't make you very secure
- That it's fine to use the same password a lot as long as it's strong – what if the website is hacked? Do you know how the website stores your password? What if they store it in plaintext?

Guilty

- Weak practices – storing passwords in the notes field on your phone, does it auto sync to the cloud, iCloud or Dropbox
- Putting them in a spreadsheet, even password protecting a spreadsheet doesn't keep the information safe.

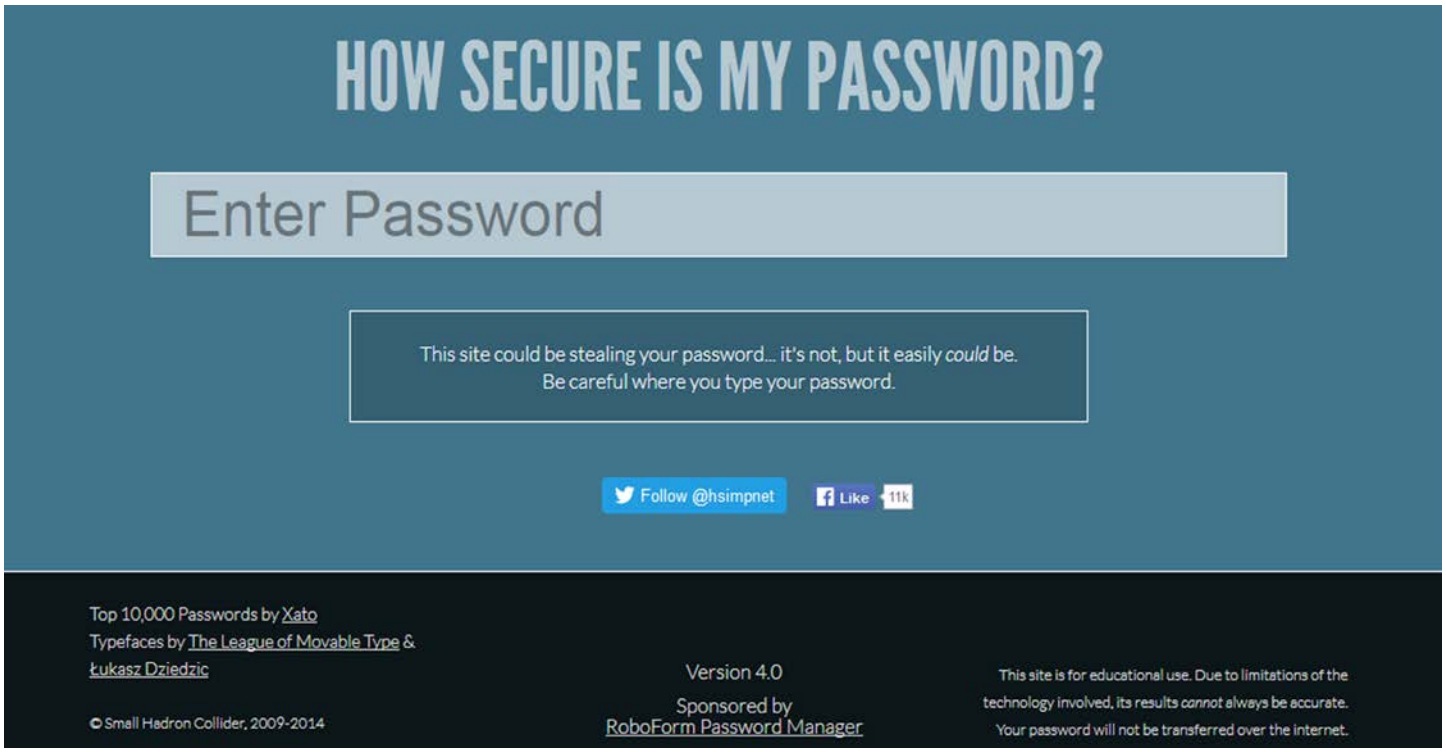
What makes a strong password?

A strong password is one that's either not easily guessed or not easily brute forced. To make it not easily guessed it can't be a simple word, to make it not easily cracked it needs to be long and complex. Super computers can go through billions of attempts per second to guess a password. Try to make your passwords a minimum of 14 characters.

Passphrase

A passphrase is simply a password, that's longer, it could be a sentence, with spaces and punctuation in it. The benefit of a passphrase is that typically they're easier to remember, but more difficult to crack due to their length. For every additional character in the length of a password or passphrase, the time it would take to break increases exponentially. Ultimately this means that having a long password or passphrase can make you far more secure than having a short one with some symbols or numbers in it.

Reference : https://www.my1login.com/resources/password-strength-test/



Check your password strength before settings up password for your own or business use

VULNERABILITY NOTES

CERT-In Vulnerability Note CIVN-2016-0061

Multiple Vulnerabilities in Cisco

Software Affected

- Cisco ACE 4710 Application Control Engine running A5 software releases up to A5(3.0)
- Cisco Nexus 2000 Series Fabric Extenders
- Cisco FirePOWER Management Center versions 5.x and 6.0.0.x

Overview

Multiple vulnerabilities have been reported in Cisco ACE 4710 Application Control Engine Command Injection, Cisco Nexus 2000 Series Fabric Extender Software Default Credential and Cisco Fire Power Management Center Unauthenticated Information Disclosure which could be exploited by an unauthenticated remote attacker to obtain information and to gain access with root user privileges.

Description

- **Cisco ACE 4710 Application Control Engine Command Injection Vulnerability (CVE-2016-1297)**

  This Vulnerability is due to insufficient validation of user-supplied input which could be exploited by a remote attacker by sending specially crafted malicious HTTP POST request with injected CLI commands inside the parameter value of POST and bypass the role-based access control (RBAC) restriction enforced by the Cisco ACE Device Manager GUI. Successful exploitation of these vulnerabilities could allow a remote attacker any command line interface (CLI) command with admin user privileges.

- **Cisco Nexus 2000 Series Fabric Extender Software Default Credential Vulnerability (CVE-2016-1341)**

  This Vulnerability exists in the Cisco Nexus 2000 Series Fabric Extender due to missing password for the root user account which is created at the time of installation and cannot be changed or deleted without impacting the functionality of the device which could be exploited by remote attackers by physically connecting to the affected device. Successful exploitation of this vulnerability could allow a remote attacker to gain access with root user privileges on the affected device.

- **Cisco FirePOWER Management Center Unautheticated Information Disclosure Vulnerability (CVE-2016-1342)**

  This vulnerability is due to verbose output returned when HTML files are retrieved from the affected device which could be exploited by remote attackers by reading the information disclosed in the files to conduct further attacks. Successful exploitation of this vulnerability could allow a remote attacker to obtain information about Cisco FirePOWER Management Center Software from the device login page.

VIRUS ALERTS : RANSOMWARE LOCKY

Ransomware - Locky is a ransomware that scramble the contents of a computer or server (associated network shares, both mapped and unmapped and removable media) and demands payment to unlock it "usually by anonymous decentralized virtual currency BITCONS".

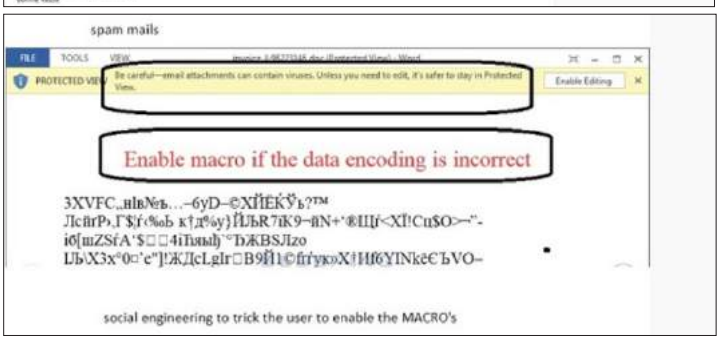
Locky Features

- Domain Generation Algorithm (DGA)
- Mapped / Unmapped Network share discovery
- Restore point deletion

The content of the original files are encrypted (renamed to .locky) using an RSA-2048 and AES-1024 algorithm. The compromised user has to pay the attacker to get the files decrypted fromthe attacker.

Propagation Methods

The primary modus operandi of Locky is via spammed emails that come with an attachment in the form of a MACRO ENABLED Microsoft Office document file with catchy subjects similar to ATTM : Invoice J-98223146 / invoice_J-12345678.doc / Rechnung-54-110090.xls



InfoSec NEWS

45-year-old woman duped of Rs 1.2 crore in matrimonial site fraud over 15 months

Kalyan: A 45-year-old Dombivli woman recently approached the Thane cyber police cell alleging she was duped of Rs 1.2 crore by a US resident whom she had befriended on a matrimonial website, and by as many as 36 of his associates, over a span of 15 months.

The main accused introduced himself as a Los Angeles-based businessman who lived in a 4BHK flat—an obvious draw in space-starved Mumbai. The accused, Robert (name changed on police request), approached the woman on the website on May 19, 2014, saying he was looking for an Indian bride as he found the country's women to be "good-natured".

In her police complaint, the victim said after declaring his intent to marry her "very soon" and winning her trust, the accused began to ask her for money citing temporary financial difficulty or an emergency. The woman believed him blindly and took several loans and even mortgaged one of her flats to "help him out" by transferring funds into various overseas accounts. Currently, the victim is using most of her earnings to repay the loans.

Representative image.

For more details :

http://timesofindia.indiatimes.com/city/mumbai/45-year-old-woman-duped-of-1-2-crore-in-matrimonial-site-fraud-over-15-months/articleshow/50952319.cms?from=mdr

Published in Times of India on 11th Feb 2016

Card cloning, fake sites test cyber cell muscle

Lucknow: Card cloning, OTP (one time password) fraud, phishing, spoofing, stalking, intrusion and non-delivery of merchandise are some of the cybercrime related complaints law enforcement agencies in the state have received in the past few years.

Latest challenge to cyber police is dealing with organised cybercrime. In November last year, an organised credit/debit card cloning gang was busted by city police.

Three employees of a Gomtinagar-based restaurant were arrested for duping at least 36 residents of the city. The gang used to copy credit card information when unsuspecting customers swiped their card on the portable machines.

The gang had attached a small skimming device on the machines. They were in touch with Mumbai and Bengaluru-based masterminds and passed on the stolen data to them. The masterminds have not been nabbed yet.

On Safer Internet Day on Tuesday, TOI puts together three novel modus operandi besides cloning that were reported this year to Special Task Force and Hazratganj-based cyber cell. Staying secure is best way to evade cybercrime, feel experts.

Fake shopping sites: STF and Hazratganj-based cyber cell have both received complaints related to fake e-commerce sites. Such complaints were not heard of in 2014 but became common last year. At least 22 city residents became victim of fake shopping site last year. Net users got attracted to unbelievable discount offers and in order to grab the deals, paid the money. The delivery never came and numbers provided on such sham portals were also found out of order. Cyber experts said gangs send mailers in person's inbox and provide link to the shopping site.

For more details :

http://timesofindia.indiatimes.com/city/lucknow/Card-cloning-fake-sites-test-cyber-cell-muscle/articleshow/50908649.cms?from=mdr

Published in Times of India on 9h Feb 2016

For any queries on Information Security
Call us on Tollfree No.

1800 425 6235

Between 10 A M to 6 P M
or give us a missed call, we will call back within 24hrs

ISEA WhatsApp Number for Incident Report

+91 9490771800

between 9.00 AM to 5.30 PM

To share tips / latest news mail us to
pmu-isea@cdac.in

Follow us on Facebook
https://www.facebok.com/infosecawarenesss

Follow us on Youtube
https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

Follow us on Twitter
https://twitter.com/CDAC_ISEA

For more details visit
www.infosecawareness.in

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.

Department of Electronics & Information Technology,
Ministry of Comunications & Information Technology,
Government of India

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
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post) Hyderabad - 500005, Telangana