Guidelines to choose web browsers

A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities. When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colour padlock symbol on the lower right corner of the browser window.

9.3 CLEARING CACHE FOR BROWSERS

Your internet browser's cache stores certain information (snapshots) of webpages you visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times. Occasionally, however your cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content. You can fix many browser problems simply by clearing your cache. This article contains instructions with screenshots on how to clear the cache for all major browsers.

Example- Clearing cache for Chrome Browsers above version 10

Step 1: Open the settings on Chrome. Click the menu icon in the upper right corner of the browser to the right. Click settings on the bottom of the menu.

Step 2: From settings, click "Show advanced settings. It's located at the very bottom of the settings section. 98

Step 3: Scroll to the privacy section and click "Clear browsing data.

Step 4: Select "Cached images and files". Uncheck all other options to avoid deleting browser history, cookies and other things you may wish to retain. Change "Obliterate the following items from" to "the beginning of time".

Step 5: Press "Clear browsing data". You are done!

Antivirus

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

Different anvirus available on the market4

bitdefender
F-SECURE
Quick Heal
Windows Live OneCare
AVG
K7 Computing
ウイルスセキュリティ
KASPERSKY
symantec.
VISION POWER
PANDA SECURITY
McAfee
AhnLab
TREND MICRO
ZoneAlarm
ca

Email Security

1. Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.

2. You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is *Tor* (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.

3. You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.

4. You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.

Guidelines for Secure Password

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basics

 Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.

- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

Tips

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the users name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody elses.
 "mItWdOtW4Me" - Monday is the worst day of the week for me.

How would a potential hacker get hold of my password anyway?

There are four main techniques hackers can use to get hold of your password:

1. Steal it. That means looking over your should when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
2. Guess it. It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
3. A brute force attack. This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. A dictionary attack. A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Password Manager
11 http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/
We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that‟s where a password manager 56

comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

6.2.1 What is a password manager?

A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

6.2.2 Why you should use it?

If you find it hard to remember passwords for every website and don‟t want to go through the „Forgot password?‟ routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

6.2.3 How does it work?

Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need.

Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don‟t have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

6.2.4 Some popular Password managers

The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven‟t decided on one, this section features the top five.

1. **KeePassX:** KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database. KeePassX uses its own random password generator, which makes it easier to create strong passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customise groups, making it more user friendly. KeePassX is

not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.

Features

- *Simple user interface:* The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.
- *Portable media access:* Its portability makes it easy to use since there‟s no need to install it on every computer.
- *Search function:* Searches in the complete database or in every group.
- *Auto fill:* There‟s no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- *Password generator:* This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- *Two factor authentication:* It enables the user to either unlock the database by a master password or by a key from a removable drive.
- *Adds attachments:* Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.
- *Cross-platform support:* It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
- *Security:* The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
- *Expiration date*: The entries can be expired, based on a user defined date.
- *Import and export of entries: Entries:* from PwManager or Kwallet can be imported, and entries can be exported as text files.
- *Multi-language support:* It supports 15 languages.

2. **Clipperz:** Clipperz is a Web-based, open source password manager built to store login information securely. Data can be accessed from anywhere and from any device without any installation. Clipperz also includes an offline version when an Internet connection is not available.

Features

- *Direct login*: Automatically logs in to any website without typing login credentials, with just one click.
- *Offline data*: With one click, an encrypted local copy of the data can be created as a HTML page.
- *No installation:* Since it‟s a Web-based application, it doesn‟t require any installation and can be accessed from any compatible browser.
- *Data import:* Login data can be imported from different supported password managers.

 Security: The database is encrypted using JavaScript code on the browser and then sent to the website. It requires a passphrase to decrypt the database without which data cannot be accessed.

 Support: Works on any operating system with a major browser that has JavaScript enabled.

3. Password Gorilla: Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.

Features

 Portable: Designed to run on a compatible computer without being installed.

 Import of database: Can import the password database saved in the CSV format.

 Locks the database when idle: It automatically locks the database when the computer is idle for a specific period of time.

 Security: It uses the Twofish algorithm to encrypt the database.

 Can copy credentials: Keyboard shortcuts can be used to copy login credentials to the clipboard.

 Auto clear: This feature clears the clipboard after a specified time.

 Organises groups: Groups and sub-groups can be created to organise passwords for different websites.

4. **Gpassword Manager:** Gpassword Manager is a simple, lightweight and cross-platform utility for managing and accessing passwords. It is published under the terms of the Apache License. It allows users to securely store passwords/URLs in the database. The added entries can be marked as favourites, which then can be accessed by right-clicking the system tray icon. The passwords and other login information shown in the screen can be kept hidden based on user preferences.

Features

 Access to favourite sites: A list of favourite Web pages can be accessed quickly from the convenient „tray‟ icon.

 Quick fill: Passwords and other information can be clicked and dragged onto forms for quick filling out.

 Search bar: The quick search bar allows users to search passwords that are needed.

 Password generator: Passwords with user-defined options can be generated with just a click.

 Quick launch: Favourite websites can be launched by right-clicking the tray icon.

5. **Password Safe:** Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on SourceForge and developed by a group of volunteers. It‟s well known for its ease of use. It is possible to organise passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic licence.

Features

 Ease of use: The GUI is very simple, enabling even a beginner to use it.

 Multiple databases: It supports multiple databases. And different databases can be created for each category.

 Safe decryption: The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.

 Password generator: Supports the generation of strong, lengthy passwords.

 Advanced search: The advanced search function allows users to search within the different fields.

 Security: Uses the Twofish algorithm to encrypt the database.

Wifi – Secuity

This chapter is about different kind of Best Practices that should be followed when using Wireless LAN.

10.1 WHAT IS WIRELESS LAN?

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable. The Wikipedia says: “Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free.”

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed. So it‟s cheap and provides same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.

5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.

10.2 MAJOR ISSUES WITH WLAN

Having said that, WLAN are also as prone to various attacks as their counterpart wired LNAs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), Deauthentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

10.2.1 Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

10.2.2 Wi-Fi at home

Using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it? Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor‟s and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. Use most secure possible encryption: The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel. 119

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

Attacks mitigated: WEP Key cracking, Sniffing, Capturing/Eavesdropping

2. Use Firewall: All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

Attacks mitigated: Fingerprinting, System compromise

3. Have a monitoring system in place: There‟s a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

Attacks mitigated: Scanning, DoS

4. Don't use default credentials: Every wireless router comes with a set of default username/password. Sometimes, people don‟t change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".

Attacks mitigated: Unauthorized access, War driving

5. Disable Auto-connect feature: Some devices or the computers/laptops have „Let this tool manage your wireless networks‟ or „Connect automatically to available network‟. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as „HotSpot‟, „SecureConnect‟, ‟GovtNetworks‟ etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

Attacks mitigated: Phishing, Sniffing, Rouge AP association

6. Don't use public Wi-Fi spots to surf sensitive websites: Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do 120

not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep [http://codebutler.github.com/firesheep/]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi.

Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked.

Attacks mitigated: Sniffing, Session Hijacking

7. Change the default SSID: Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

Attacks mitigated: War driving

8. Restrict access by assigning static IP addresses and MAC filtering: Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

9. Turn off your router when not in use: Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

Due to the nature of activity and criticality of information, it is very important that Corporate / Enterprise networks have a higher degree of security.

The following are good to have:

- Defining an adequate organization wide Information Security policy & procedures for wireless network
- SSID‟s should not be associated with the organization, AP vendor or any other related information which would be easy to guess or associate with the current organization
- Enable WPA2 Enterprise encryption with RADIUS authentication and use of EAP protocol like EAP-TTLS, TLS etc.
- Implementation of PKI infrastructure. CA signed certificates to authenticate the server to client and vice versa
- Filtering of clients based on unique identifier like MAC Address
- Isolated „Guest‟ wireless network with no interface / connection to the corporate network
- Limiting the radius of Wi-Fi network by reducing the power output of the AP
- Allocating IP Address to the employee and guest machines only after successful authentication
- Periodically changing the keys & passwords
- Use of VPN while accessing corporate information from Public Wi-Fi network
- Client side utilities like DecaffeintIDcan help in detecting changes in ARP table and serve as common man‟s IDS to protect against attacks like „hole196‟ and DoS.

- Implementation of Wireless IDS. Wireless IDS is a new concept. The key features of Wireless IDS are:
- Prevention against Rogue AP‟s
- Detection & prevention against DoS attacks
- Assistance in locating the approximate physical location of the attacker
- Assistance in enforcing the Organization‟s Information Security policy on wireless networks
- Detection of use of scanning tools like Kismet & NetStumbler