UNIT-3

IT Security Tools & Techniques

Learning Outcomes
By the end of this unit the learner will be able to:
Understand the most effective cyber security tools and techniques Discuss the importance of proactive cyber security Set secure passwords with confidence

Unit 3

IT Security Tools & Techniques

Prevention and Defenses

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

Authentication

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber-crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process.

It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network.

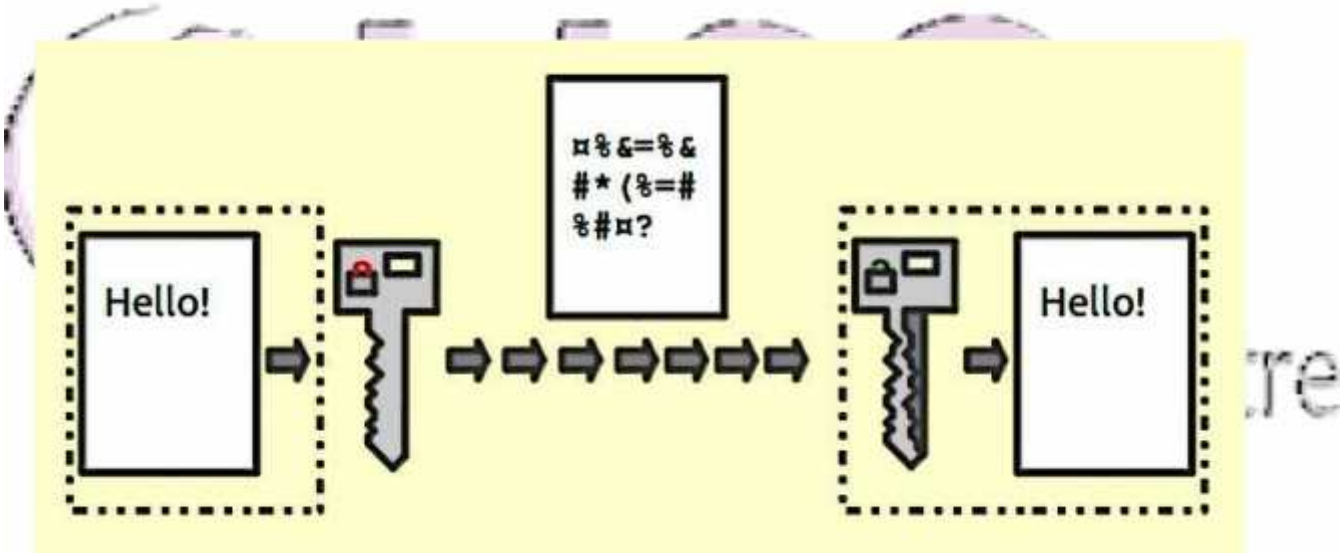
The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization.

Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk. Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication system is used

which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use VPN(Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.

Encryption

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.



Source Wikipedia: Figure 3.1: Encryption

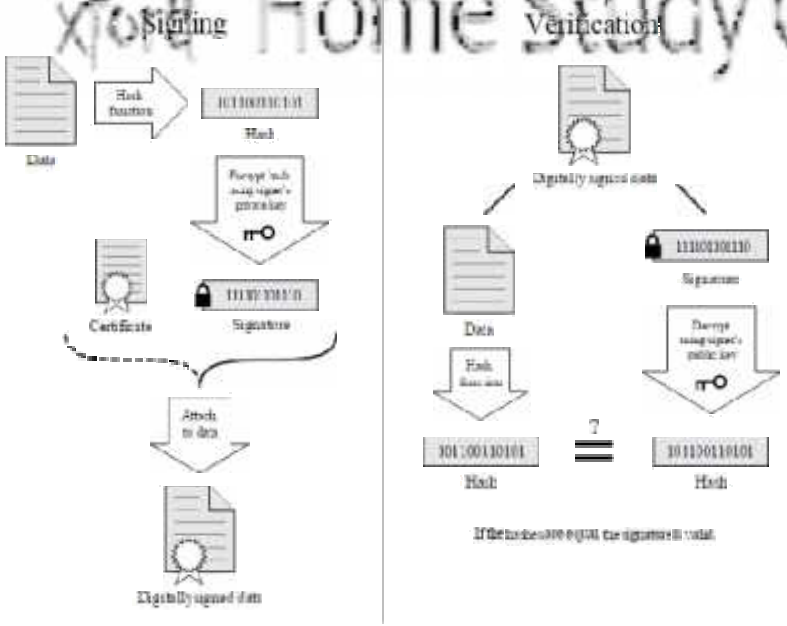
In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse‟s two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B‟s public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As

soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

Digital Signatures

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender.

Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original senden, is required for this purpose.As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.



Source Wikipedia: Figure 3.2: Digital signature

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.

Figure 3.3: Different anvirus available on the market

Firewall

It is a hardware/software which acts as a shield between an organization‟s network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.

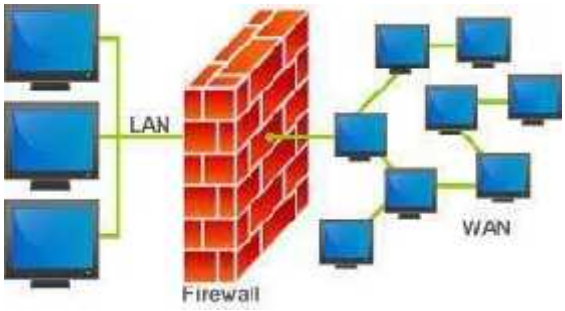


Figure 3.4: Firewall

There are two types of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization‟s network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly.

A firewall can be implemented using hardware as well as software or the combination of both.

- **Hardware Firewalls:** example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- **Software Firewalls:** These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.

In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow “rules” and “policies” and based on these defined rules the firewalls can follow the following filtering mechanisms.

- **Proxy:** all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- **Packet Filtering:** based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- **Stateful Inspection:** rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

The firewalls are an essential component of the organizations‟ network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

Steganography

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

- There are various free softwares available for Steganography.
- Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

Generating Secure Password

Guideline for setting 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.

Using Password Manager

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.

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

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.

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.

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.

Guidelines For Safe Internet Browsing

Safe Browsing

Internet security is a matter of great concern for internet users. It is important to know if a website is secure or not while surfing the internet19. 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.

How do I know if a website is secure?

Some web sites use a secure connection between the web site and your browser. This may be important to you, for instance, if you want to pay online for a product or a service and have to enter credit card information or other personal information. To know if your browser is viewing a secure website, you can look in the lower right part of the window. There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon). If you see a yellow padlock icon, the web site you are viewing is a "secure web site." If the box is empty, the web site does not have a secure connection with your browser.

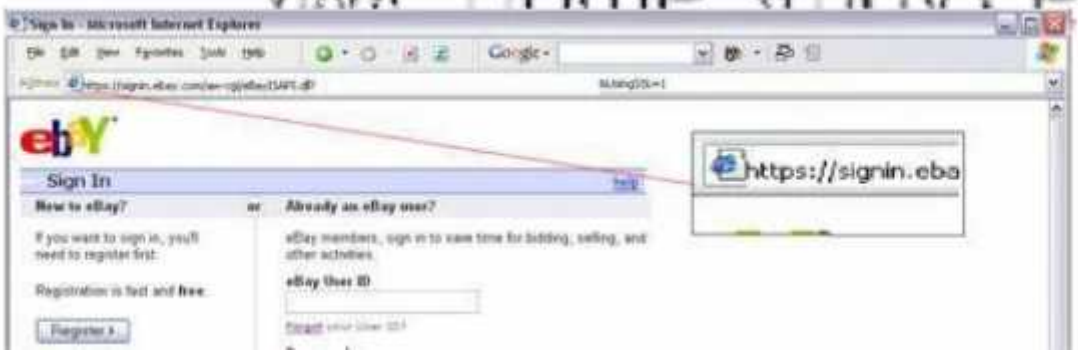


Fig. 3.5

Tips For Buying Online

Shopping online can be cheaper and more convenient for you and for businesses. However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

I. Pay securely: Don‟t make any payment unless:
   - You are on a secure website, and
   - You can make a secure payment.

This will protect you against fraud and unauthorised credit card transactions. A secure website address will always:

- begin with „https://‟, not „http://‟
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

Only make a payment if you can see both of these things. Never give out your bank account details, credit card number or other personal details if you are not certain that the business is a reputable trader.

II. **Know the business:** Only buy from websites you know and trust. Check that the company has a physical street address and landline phone number. If the company operates from overseas, you might have trouble getting a refund or repair.

III. **Know the product:** Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.
- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

IV. Check the full cost: Be aware of the full cost of your purchase. Additional costs may include:

- currency conversion
- taxes
- postage and delivery fees
- packaging.

It might end up being cheaper to buy the product at a local shop.

V. Protect your privacy: Only buy online if you are comfortable with a business‟s privacy policy. Do not give out information unless they require it to complete the sale. Remember, if a deal sounds too good to be true, it probably is.

VI. Keep records: Always write down any reference numbers and print out copies of:

- the order form (both before and after you confirm the order)
- receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.

The charges may be converted from another currency.

VII. Online auction sites: Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers. This should be your first step to resolve a dispute if:

- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description. The eBay website has an example of this facility.

Wireless Security

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

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.

Figure 3.6: A typical Wireless network

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.

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.

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:

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

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

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 Email and Social Media Security

Safe Browsing Guidelines For Social Networking Sites

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

General Tips on using Social Networking platforms safely

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account.

Given below are some of the general tips on using social media.

Always ask the questions:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?
- Will my contacts mind if I share information about them with other people?

- Do I trust everyone with whom I'm connected?
- Always make sure you use secure passwords to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default privacy settings offered by the social networking site, and how to change them.
- Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine.
- Access social networking sites using https:// to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.
- Be careful about putting too much information into your status updates – even if you trust the people in your networks. It is easy for someone to copy your information.
- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly careful when integrating your social network accounts! You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

Posting Personal Details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

Friends, Followers and Contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

Status Updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about

their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

Sharing Online Content

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

Revealing your Location

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

Sharing Videos and Photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

Instant Chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure).

It is more secure to use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

Joining and Creating Groups, Events and Communities

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

Email Security Tips

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.
5. Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.
6. Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

Smartphone Security

Introduction

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wi-fi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks. For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

Smartphone Security Guidelines

Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

A simple exercise can help illustrate this:

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find: - Pictures of loved ones (~5 pictures) - Identification cards (driver's license, membership cards, social security cards) - Insurance and health information (~2 cards) - Money (~5 bills) - Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to

restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

Specific precautions related to common uses of smartphones.

Platforms, Setup and Installation

Platforms and Operating Systems

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (FOSS) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as GPS or wireless networking capacities.

Feature Phones

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for security applications or improvements. We do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

Branded and locked smartphones

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

General Setup

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

Installing and updating applications

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you should look for alternative applications with appropriate access and rights.)ites. Some users may want to consider these alternative sites to minimize online contact with Google.

Communicating Securely(Through Voice and Messages) with a Smartphone

Secure Voice Communication

Basic telephony

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

About eavesdropping: Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

- Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.

- If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.
- Make sure that any person with whom you communicate also employs the safeguards described here.
- In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

About interception of calls: Typically, encryption of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications.

It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones.

Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place26. Using Internet through your Smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using VoIP and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well

Here we list a few tools and their pros and cons:

Skype

The most popular commercial VoIP application, Skype, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections.

Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

Other VoIP tools

Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate.RedPhone is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use, RedPhone uses your mobile number as a way to identify you to your contacts.

Unfortunately, this makes it more difficult to use RedPhone without a functioning mobile service plan, even on devices capable of using WiFi to connect to the Internet. RedPhone also uses a central server, which puts the administrators of the service in a powerful position by allowing them to see much of the meta-data related to your encrypted VoIP calls.

CSipSimple is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different VoIP services.

SMS

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

Securing SMS

TextSecure is a FOSS tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. TextSecure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to tamper with the contents of a message. In our TextSecure hands-on guide we explain in detail the features of this tool and how to use it.

Sending Email from your Smartphone

In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is

generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

- Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
- If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands.

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encrytpion key-pair (using APG) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

Through Wi-Fi or Mobile Data

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator.

Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers.

In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

Further Reading:

- ✓ ***CYBER SECURITY LAW, CYBER SECURITY LAW, by PAVAN DUGGAL Jan 17, 2019***
- ✓ ***How to Become a Cyber-Security Analyst: Phase 1, Paul Oyelakin, Sep 30, 2018***