BUSINESS NEED FOR SECURITY

Open Wi-Fi hotspots- Threats and Mitigations

By
Renuka Muppavarapu

Table of Contents

I. Introduction:

Users must update to better security measures while connecting to open Wi-Fi hot-spots as they turn out to be more risky than useful. It would come across as a cause of concern to know that 42% of wireless 802.11 access points come with no security mechanisms. By this we mean they are not even protected by WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) [1]

Free Wi-Fi and good speed can be the best thing that can happen to a person sitting leisurely at a public place. If a coffee shop or a restaurant had an open Wi-Fi hotspot, more than 50% of the people present there would connect to it to carry out activities through their smart phones or laptops or any Wi-Fi supporting gadgets. It is sheer convenience and a cost effective measure to browse internet through a free hot spot. In most hotels or restaurants, one of the most important aspects people check before entering is whether free Wi-Fi is being provided or not.

The below picture describes the need and usage of Wi-Fi by users while in transit and in accommodation:

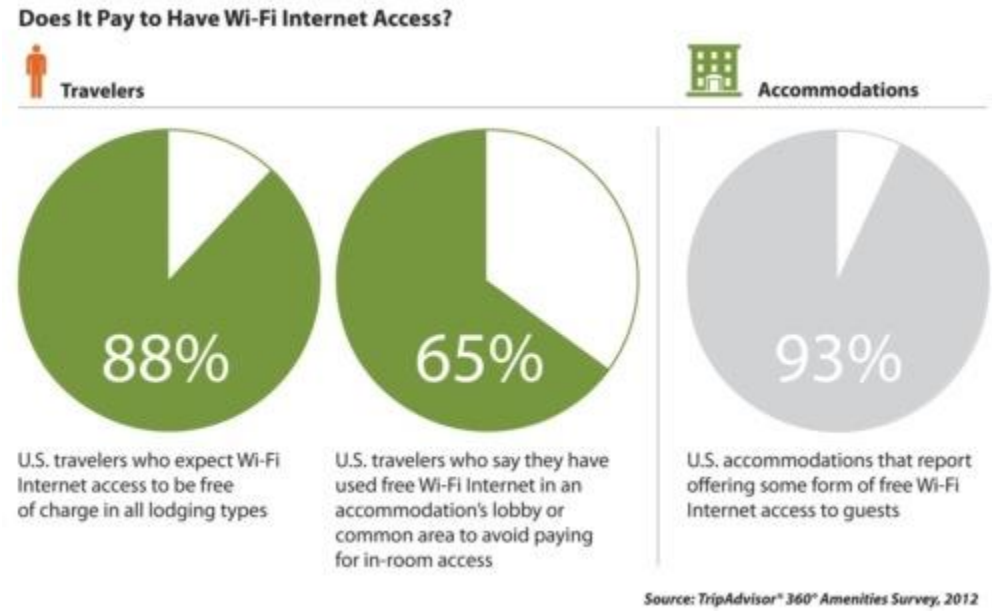

Figure 1: Usage of Wi-Fi in transit

Source: This above illustration is adopted from Trip advisor 360 Amenities Survey, www.gadling.com

When an employee connects to the open hot spot and sends an email to a colleague, he is keeping a lot of information, money, business, also probably his job at stake. It is because someone sitting next to the employee would easily pass as just another visitor but might be a professional hacker who is spying on every bit of information transmitted through their gadgets to misuse it. Same case would be with another person casually browsing the net or paying bills or shopping online. How horrifying would it be to know that your credit card information is being stolen or misused by an attacker who is sitting right across your table? Open Wi-Fi proves to be a necessary evil. Even though nobody was shoulder surfing, the hot spot vendor is a highly trusted source, users are becoming victims of serious cybercrimes. There are many ways a hacker can pose a threat to Wi-Fi hotspots.

One very dangerous form of attacks is evil twins. A user isn't even aware but he would connect to a fake hot spot exposing his passwords and a lot of other and private and sensitive information. Certain measures are to be taken to prevent a user's information from being illicitly stolen. We are soon going to expand on what these measures are, why they need to be taken and what the consequences of not incorporating this into our system are.

II. Threats posed to business professionals by open Wi-Fi hotspots

Most employees of an organization have their official email accounts on their phone. If any person traversing from one point to another notices an open Wi-Fi connection which enables them to connect to their work environment or social networking sites, he/she would be tempted or would find the need to connect to it. In an insecure environment where there might be threats posed to the information transmitted over the Wi-Fi, the information assets of Wi-Fi users are highly at stake.

Let us consider a scenario where a person is sitting in a public bus. If an instance occurs where they have to connect to their office environment which requires a good bandwidth for smooth functioning and free Wi-Fi with a good speed is present, how many people would actually think twice before connecting to it? Even if half of the people connect to that Wi-Fi point, an attacker can use various methods to steal sensitive information and can cause a lot of damage to the information. Critical and confidential data of an organization can be handily exploited.

A. Most common threats to devices connected to open Wi-Fi hotspots

1. Types and description of threats.

- Sniffing: An attacker sniffs the packets that travel between two systems by monitoring network traffic and in this way he can gain access to the user login credentials and other sensitive information that flows over the network. [2]

- Spoofing: An attacker sends messages to a computer with an IP address indicating that the message is coming from a trusted host. These attacks can be implemented easily and they can have an impact on the network performance.[3]

- Side-jacking: An attacker sniffs packets from a network and with this he can steal the session cookies. He uses these cookies to authenticate to a web server. Websites usually use the HTTPS (Hypertext Transfer Protocol Secure) protocol only at the time of log in to safeguard the user name and password but later they switch to HTTP (Hypertext Transfer Protocol). In this process, the cookies still get sent to the server over the unsecure HTTP protocol and this is when a hacker can sniff information. [4]

- Rogue access points*:* These are access points that appear as legitimate access points but may be fake ones created by an attacker. These points trick users into connecting to the fake access points. Once connected to the rogue access point, the user traffic is redirected through the fake access point and is analyzed by the attacker. This falls under the category of MITM (Man in the Middle) attacks. [5]

2. Basic security measures:

There are certain measures that need to be taken before a user connects to a hot spot, to avoid being a victim of the above mentioned attacks. They are as follows:

- After disconnecting from an unknown hotspot, it is better to scan the system if any virus has been induced into it, so that it can immediately be fixed before any damage is done.

- Websites that have HTTPS encryption are safer to use so other websites need to be used cautiously before entering sensitive information.
- Users need to beware of rogue access points because the names of these rogue access points seem very similar to the legitimate access points.
- A user needs to make sure that the firewall is turned on and he/she need to protect themselves from attacks from virus attacks by installing antiviruses.
- While connecting to a public hotspot like in coffee shops or restaurants, the user needs to check with the vendor whether the hotspot is a legitimate one.
- It is better to change the settings of your Wi-Fi access to disable automatic reconnection to a Wi-Fi network because most evil twins use this vulnerability.
- Easy passwords make it easier for an attacker to crack an account. So a strong password which has upper case, lower case, symbols and alphanumeric characters must be set to make sure that it is not easily cracked by brute force or dictionary attacks.
- Never store the passwords or any important information on shared folders.
- It is not safe to access banking applications while connected to a public hot spot.
- Using a virtual private network reduces the chances of loss of sensitive data to a great extent. [6]
- Wireless network must be turned off when it is not being used [7]

B. Evil Twin

1. What is an evil twin?

An evil twin is a fake access point with copies the identity of a legitimate access point. Once a user connects to a Wi-Fi network, that network is added to the list of his preferred networks. This is a feature supported by all the recent operating systems. An attacker disconnects a user from the legitimate access point and the user's device usually automatically connects to the fake access point. This happens because, the SSID and network name of the evil twin is same as that of the legitimate SSID and network name and the signal of the rogue access point is stronger than the actual access point. [8]

When the user is disconnected successfully, the system verifies the preferred network list. As the name of the network is same, it connects the user to the fake (evil twin) access point.[9] Once a connection is established, the password that a user enters

will automatically be stored in the data base of the attacker because of the configurations of the evil twin access point. [1]

Below a normal access point scenario is illustrated where a user is connected to a legitimate access point:

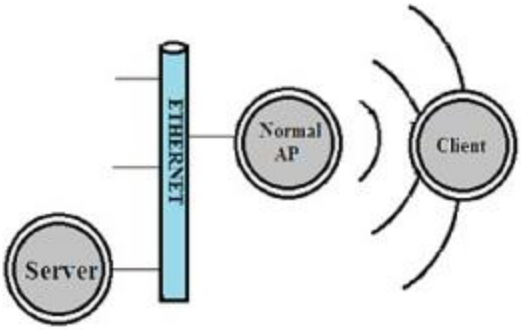

Figure 2: Normal access point
Source: This figure is adopted from Dr. Volodymyr Lysenko: Proceedings of the 7th International Conference on Information Warfare and security

When a user is connected to a rogue access point/evil twin, an evil twin access point scenario occurs.

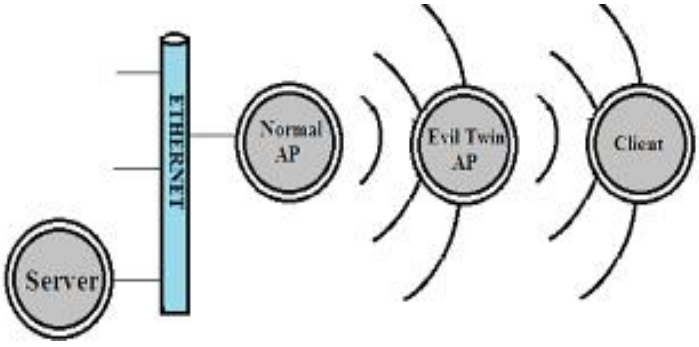

Figure 3: Evil Twin Access point
Source: This figure is adopted from Dr. Volodymyr Lysenko: Proceedings of the 7th International Conference on Information Warfare and security

2. Effects of evil-twin attack on the end user.

Once a user connects to an evil twin, an attacker can obtain access to the:

- Wi-Fi password
- Email accounts
- Credit/debit card information
- Social networking sites
- An attacker can also control which websites appear to the user and which do not.

III. The repercussions of lack of a sound security for the Wi-Fi

A. The after-effects of being a victim of cyber-crime.

1. Loss of money to restore the system to its original state:

If an employee of an organization connects to an evil twin, an attacker can successfully exploit the hot spot. To sectors of organizations where data is the most important asset, misuse of data could prove to be fatal.

For example, consider a scenario where an employee working for a start-up e-commerce company is sharing a database of user to another employee and he is connected to the evil twin while sharing the file, the attacker can obtain the valuable data and misuse/modify it. This would incur a huge financial loss to the company and damage the brand reputation.

2. Loss of time in retrieving back the lost/damaged/misused data:

Once an organization's reputation is affected, its business is also impacted. To bring back the position of the organization in the market, it takes a lot of security measures, policy changes, money, due care, due diligence, increase in the work productivity to be in par with the other companies in the market again.

IV. Measures to mitigate evil twin attacks

The following measures need to be taken by organizations/employees/laymen to safeguard their data from threats like evil twin attacks.

A. WPA-PSK method:

In this method, the client gets a secret passcode through a method previously agreed upon. This could involve distribution of the passcode through mobile, tokens etc. This method holds good for mitigating evil twin attacks that occur in large and medium sized enterprises as they can afford the cost of implementation. But for public open Wi-Fi hotspots or small sized enterprises, this might not be the best solution.

For small sized enterprises, a possible method to mitigate evil twin would be by implementing the Trust on first use (TOFU) model. [10] But this has setoffs like being prone to man in the middle attacks. [11]

B. Using a Virtual Private Network:

If a user frequently connects to public hot spots, a good option would be that they sign up for a VPN service. A VPN service ensures that all the data that travels in the network is encrypted. [12] It acts as a physical barrier between the user and the web. This could prove to be an efficient and cost effective solution. Even if an attacker tries to snoop on the unencrypted traffic between the server and the internet, he cannot associate which information pertains to which user because it is all going from a single VPN server. The figure below shows the information transfer between a user and the web through a VPN.

Figure 4: Data transmission through VPN
Source: This figure is adopted from Amadou Diallo: "Want Privacy on the Internet? Then You Need a VPN" http://www.forbes.com/sites/amadoudiallo/2014/03/07/want-privacy-on-the-internet-then-you-need-a-vpn/

The main use of a VPN is to connect to a remote network securely. This is used by most of the organizations to provide access to the work environment, files, applications and other resources which are specific to the organization without the security being compromised. It is also expedient when an organization has its work places spread across the globe. Servers and networked resources are shared by companies with the help of a VPN.

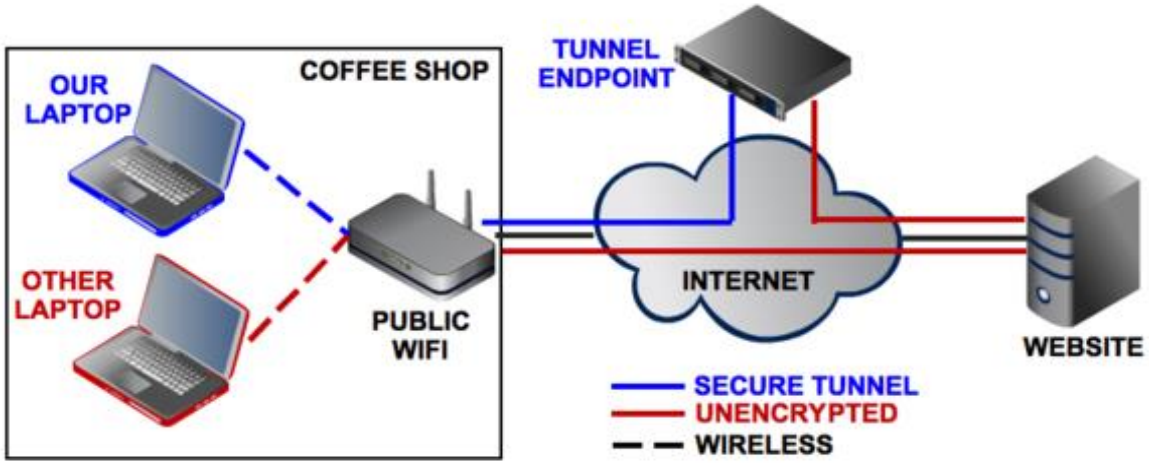

Figure 5: Traffic being tunneled
Source: This figure is adopted from Steven Andres: "How to set up a Secure Web Tunnel" http://www.pcworld.com/article/197725/how_to_set_up_a_secure_web_tunnel.html

It is a boon to users who connect to public Wi-Fi because there might be rogue access points created in the vicinity of an authorized Wi-Fi connection in order to trap users. This ends up establishing a connection between the user's device and the fake access point. Networking protocol that is used while building a VPN is one of the important aspects to be considered. There are four protocols which are widely in use: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec), Secure Sockets Layer (SSL) and Open VPN. An analysis of the strengths and weaknesses of each protocol based on its performance, stability, link quality makes

it easier to determine which protocol can be chosen for the VPN. This in turn enables a user/vendor to determine the specifications to look for, while selecting the right VPN and protocol for their network. [13]

Point-to-Point Tunneling Protocol: It is one of the least secure methods. But it is widely used because it is supported by all operating systems. Point to point protocol was extended into point to point tunneling protocol. This was developed by Microsoft and is compatible with any version of Microsoft windows. [14] There are two different types of packets that PPTP uses to establish a VPN connection. One is the generic routing encapsulation and the other is the PPTP control message. Neither of these methods provide encryption of data or authentication hence this protocol must be used in collaboration with other security methods. For customers who do not want to install additional software for implementing VPN, PPTP is a good option because most of the customers use Microsoft Windows or Mac OS. There is not much protocol overhead when we use PPTP and also it is cost effective, hence a best option to choose when cost is a constraint.

Layer 2 Tunneling Protocol (L2TP): It is better than PPTP in terms of security but the set up or usage of PPTP is easier than L2TP. Internet Protocol Security (IPsec) and L2TP are almost on the same lines when we consider its complexity or security. L2TP supports an encapsulation of a data link layer frame into a packet at the transport layer. In this way, transmission of data packets through the internet can be accomplished. L2TP is usually combined with IPsec by adding the header of IPsec in front of the L2TP header. But we need to keep in mind that combining two protocols will result in a protocol overload. This is not a suitable option for mission critical applications as it does not include mechanisms for data privacy. [15]

SSL VPN: On the other hand, Secure Sockets Layer (SSL) Virtual Private Network is one of the most widely accepted methods chosen to extend network resources to a user who is located in a remote location. It uses Internet Protocol tunnels to establish an encrypted communication between networks. As discussed, it is the most widely accepted for the following reasons.

- It does not require a dedicated client for running it which is why it is often called clientless.
- It is more user friendly and the connection is established through a web browser.

- It is more reliable than the other three methods discussed above i.e. PPTP, L2TP, and IPsec because the data transmitted is encrypted.

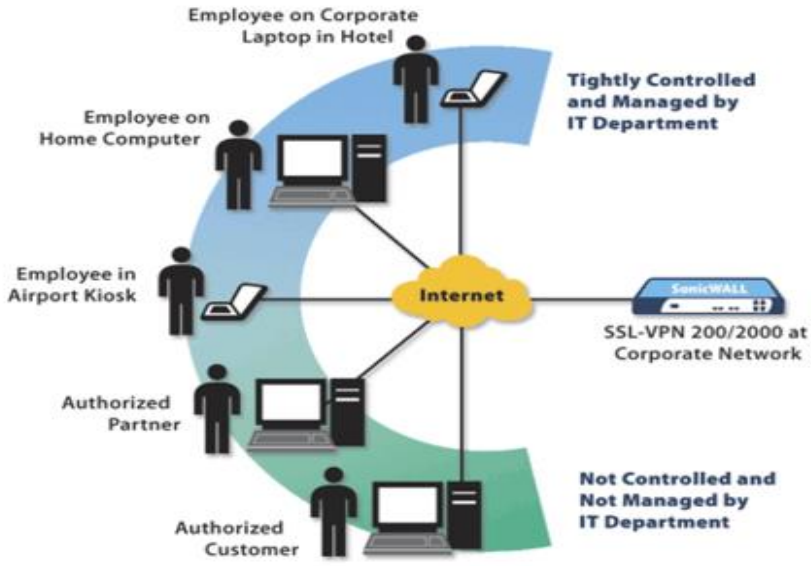

Figure 6: SSL VPN
Source: This figure is adopted from Eric Geier: "How any why to set up a VPN today"
http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

Open VPN: It is based on SSL code and it is free from connection issues. Unlike SSL VPN, to use Open VPN, a client needs to be installed because Mac OS X, Windows or mobile devices do not originally support it. This is highly secure. Open VPN uses TCP or UDP protocols to establish the connectivity. The encryption algorithms use by Open VPN are: 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard), BF (Blowfish), IDEA (International Data Encryption Algorithm). [13]
For example: Cisco is supplying VPN services keeping in view various factors by offering deployment flexibility, network access, clientless access, granular control, seamless connectivity, organized performance, management flexibility and optimum costs. The Cisco ASA 5500 Product Family targets all kinds of users and provides a user to choose from a wide range of products which is best suited for a requirement. The below figure illustrates the models developed by Cisco.

Figure 7: Cisco ASA 5500 Series Products

Source: This above illustration is adopted from Cisco," Cisco Secure Remote Access Cisco ASA 5500 Series SSL/Ipsec VPN Edition" http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_brochure0900aecd80402e39.html

Specifications for Cisco ASA 5500 Series Adaptive Security Appliance Models [16]

Platform	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40	Cisco ASA 5585-S10	Cisco ASA 5585-S20	Cisco ASA 5585-S40	Cisco ASA 5585-S60
Maximum VPN throughput[1]	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Maximum concurrent AnyConnect or clientless VPN sessions[1]	25	250	750	2500	5000	10,000	10,000	5000	10,000	10,000	10,000
Maximum concurrent site-to-site and IPsec IKEv1 VPN sessions[1]	25	250	750	5000	5000	10,000	10,000	5000	10,000	10,000	10,000
Profile	Desktop	1-RU	1-RU	1-RU	1-RU	4-RU	4-RU	2-RU	2-RU	2-RU	2-RU
Stateful failover	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPN load balancing	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Shared VPN License Option	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] Devices include a license for two Premium VPN users for evaluation and remote management purposes. The total concurrent IPsec and SSL (clientless and tunnel-based) VPN sessions may not exceed the maximum concurrent IPsec session count shown in the chart. The SSL/IPsec IKEv2 VPN session number (clientless or AnyConnect client) may also not exceed the number of licensed sessions on the device. The ASA 5580 supports greater simultaneous users than the ASA 5550 at comparable overall SSL VPN throughput to the ASA 5550. VPN throughput and sessions count depend on the ASA device configuration and VPN traffic patterns. These elements should be taken in to consideration as part of the capacity planning. Based on the user's requirements the configurations can be made.

While connecting to a public Wi-Fi hotspot, there are other VPN products that can be used, with zero no cost for non-commercial purposes. They are as follows: [17]

- LogMeIn Hamachi
- UltraVPN
- AlonWeb
- Hotspot Shield
- CyberGhost
- Ultrasurf

C. Awareness of cyber security

One of the simplest ways to ensure prevention of attacks on Wi-Fi security is to create awareness in the employees of an organization. We reflect upon the notion that Humans are the security's weakest link in this aspect. Employees must be made well aware of the basic threats, attacks and the measures to be taken to mitigate the attacks that can be posed when accessing internet through Wi-Fi. This reduces the chances of attacks to a great extent and indirectly saves a lot of money for the organizations they work for, which would have otherwise been lost in the process of restoring the attacked assets.

The Department of Homeland Services and other federal agencies proposed certain measures for small and medium sized enterprises as a basic step to improve cybersecurity of their organizations. [18] They can be expatiated as follows:

- Across the organization, automate patch deployments to safeguard against vulnerabilities.
- Hide your Wi-Fi network and secure the data by encrypting it.
- Invest money in data loss protection software.
- Protect all the public facing websites including the login and logout pages.

National Cyber Security Awareness Month (NCSAM)

The national cyber security division which is within in the Department of Homeland Security and the National Cyber Security Alliance (NCSA, a non-profit organization) aims at engaging public and private sectors in events which will spread awareness about cybersecurity and educate citizens to ensure an increase in resilience and build a better cyber infrastructure. It celebrates the National Cyber Security Awareness Month every October since 2004. Various events are organized for spreading cybersecurity awareness in the year 2014 which include:

- Promoting Online Safety with campaigns such as the “Stop.Think.Connect” campaign which is explained below
- Secure Development of IT Products
- Critical Infrastructure and the Internet of Things
- Cybersecurity for Small and Medium-Sized Businesses and Entrepreneurs
- Cyber Crime and Law Enforcement [19]

The “Stop.Think.Connect” campaign was started in 2009, to bring cybersecurity into the spotlight. The meaning of Stop Think and Connect in this context is as illustrated in the figure below:

Figure 8: Stop. Think. Connect campaign
Source: The above figure is adopted from Department of Homeland Security, "Stop.Think.Connect." http://www.dhs.gov/stopthinkconnect

D. Introducing the basics of cyber-security to students at an earlier age.

The majority of the user base connecting to the open Wi-Fi hotspots is students or teenagers; so if the need for cyber security and measures that are to be taken is introduced to youngsters at an earlier age, it helps in safeguarding their private data there by reducing the risk of it being attacked.

Considering the importance of imparting cybersecurity knowledge to students, the teachers and school administrators must build a platform which creates a pragmatic approach towards security education. Without making additional concepts a burden, institutions must set up workshops or fun activities to reach out to students of various backgrounds. This can be achieved by base lining their knowledge on cybersecurity and presenting real-time thought provoking scenarios to trigger their interest in improving their awareness in the field of cybersecurity. [20]

To reach out to the global audience, the International Information System Security Certification Consortium (ISC2) has a Global Academic Program (GAP) which ties up with university partners to impart skills to promote the growth of information assurance professionals. [21]

V. The perks of upgrading to stronger security measures as mentioned above:

A. Increases the productivity of an organization and reduces avoidable expenses.

The cost, resources and time that is invested in retrieving the organization's position to normalcy after an attack can be invested in increasing the work productivity of a company. This would raise the organization's position in the market by showing substantial profits by implementing the above mentioned methods.

B. Directly beneficial to end-users as their private data is kept private and unaffected.

In the end, when information assets are lost, the end user is the sufferer, be it in terms of importance of information directly to the user or indirectly to the organization. So if the necessary security measures are taken, there would be lesser need to worry about the assets being stolen or misused.

C. Works towards building a better and a robust security system throughout.

People, data, software, hardware, networks, procedure are the components of security system. When all these components are individually secured, the whole security system is secured and this makes it close to impossible for any active, passive, insider or outsider attacks to occur. [22]

VI. Conclusion:

The recent explosion of free Wi-Fi being provided at public places has become a necessary evil to the users. Inevitably, the number of people who connect to open unencrypted Wi-Fi hotspots are exponentially increasing keeping in view the business needs and the convenience it renders. [23] So when a user connects to an open hotspot he is disposed to facing threats such as evil twin attacks which a hacker executes by

creating a fake access point with an illegitimate SSID which is similar to the legit network. Once victimized by an evil twin attack, the data, sensitive information, privacy, economy is all at stake. To mitigate and prevent ourselves from being attacked by an evil twin, certain measures have been proposed, which include safeguarding the hotspot by using a virtual private network and spreading awareness and imparting cyber education in the right direction to understand the importance of cybersecurity. [24] By implementing simple methods as discussed in this paper, we can mitigate threats such as evil twin attacks to a large extent and contribute towards building a safe and resilient cyberspace which in turn impacts our daily lives and business economy.

VII. References:

[1] Kevin Bauer, By Harold Gonzales, and Damon McCoy, Mitigating Evil Twin Attacks in 802.11, IEEE Dec 2008

[2] By Ansari. S, Rajeev, S.G., Chandrasekhar, H.S. Packet sniffing: a brief introduction, IEEE Jan 2003

[3] Jie Yang ,Yingying Chen , W. Trappe , J. Cheng, Detection and Localization of Multiple Spoofing Attackers in Wireless Networks, IEEE Issue No.01 - Jan. (2013 vol.24)

[4] Kumar.V, Three Tier Verification Technique to foil session sidejacking attempts, IEEE Nov.2011

[5] Srilasak, S., Wongthavarawat, K.,and Phonphoem A, Integrated Wireless Rogue Access Point Detection and Counterattack System, IEEE April 2008

[6] "Ten Tips for Public Wi-Fi Hotspot Security" *http://www.pcmag.com/slideshow_viewer/0,3253,l=254315&a=254312&po=3,00.asp*, PC Magazine, (accessed October 16, 2014)

[7] Public Wireless Network*, http://www.microsoft.com/security/online-privacy/public-wireless.aspx* (accessed November 13, 2014)

[8] Dr.Volodymyr Lysenko, Proceedings of the 7th International Conference on Information Warfare and security,22 march, 2012

[9] Sachin R. Sonawane, Sandeep Vanjale, Dr.P.B.Mane, A SURVEY ON EVIL TWIN DETECTION METHODS FOR WIRELESSLOCAL AREA NETWORK, INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING& TECHNOLOGY (IJCET)Volume 4, Issue 2, March – April (2013), pp. 493-499

[10] Gonzales.H , Bauer.K, Lindqvist.J,McCoy.D, Practical Defenses for Evil Twin Attacks in 802.11, IEEE Dec. 2010

[11] S.S. Farrell, R.Wenning, B. Bos ,M. Blanchet Viagenie, H.Tschofenig, A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT), *https://www.w3.org/2014/strint/draft-iab-strint-report.html*, 6 May 2014(accessed November 11, 2014)

[12] Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7, 2002

[13] Jaha, A.A., Ben-Shatwan.F, Ashibani.M Proper Virtual Private Network (VPN) Solution Private Switching Systems and Networks, 1988., International Conference on Date of Conference:21-23 Jun 1988

[14] Eric Geier, "How and why to set up a VPN today" *http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html* (accessed November 9, 2014)

[15] Thomas Berger, “Analysis of Current VPN Technologies”, First International Conference on Availability, Reliability and Security, April 2006, p.8 pp. Date of Conference: 20-22 April 2006

[16]Cisco, “5500 series next generation firewalls” *http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_brochure0900aecd80402e39.html* (accessed November 4, 2014)

[17] Sam, Tech Hail, *"http://www.techhail.org/internet/20-best-free-secure-vpn-proxy-services/4360*" (accessed November 10, 2014)

[18] Phyllis Schneck, Improving Cybersecurity for Small and Medium-Sized Businesses, *http://www.dhs.gov/blog/2014/10/24/improving-cybersecurity-small-and-medium-sized-businesses* (accessed November 10, 2014)

[19]National Cyber Security Awareness Month (NCSAM) *http://www.staysafeonline.org/ncsam/* (accessed 14 November, 2014)

[20] Safe Online Surfing, The Federal Bureau of Investigation*, https://sos.fbi.gov* (accessed November 08, 2014)

[21] (ISC) ² Global Academic Program, *https://www.isc2.org/global-academic-program/default.aspx* (accessed November 12, 2014)

[22] Michael E. Whitman, Principles of Information Security, 4th ed. – Chapter: Introduction to information security

[23] Public Wi-Fi Risks and Why You Don't Have to Fear them, *http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks* (accessed November 11, 2014)

[24] Cybersecurity Overview, Homeland Security *"http://www.dhs.gov/cybersecurity-overview*" (accessed November 14, 2014)