



## Research Paper

---

# Managing security risks in wireless web services

Accepted 11<sup>th</sup> November, 2021

### ABSTRACT

Over the last twenty years, the Internet has become highly interactive and is not merely a static repository of websites, which allows its users to interact proactively. The functions and tasks of the Internet have evolved during this twenty-year period, such that it is no longer a rudimentary collection of websites. The Internet empowers individual users to explore it in an exponentially greater capacity than in years past. In this study, we will consider the issues of security and trust in IoT and local cloud interfaces. Additionally, the security, requirements of M2M services and security solutions for the internet are analyzed, and their ineffectiveness is discussed.

Alaa AL Saeed

Management Information Systems, Bowie  
State University, United States.

E-mail: alaa.adnan1990@hotmail.com.

**Key words:** Internet, computers, M2M services, cloud interfaces, WLAN, WEP, system, wireless networks, management, MAC address.

---

### INTRODUCTION

Web applications are using personal information of users for various purposes. Email accounts for instance, such as Google, yahoo, Hotmail, and other accounts require personal information that should not be available for public use. Likewise, the issue of personal information gets complex when it comes to the financial account data of users. As many banks, insurance companies, and financial institutions provide services to its customers online, then in exchange they need personal information. Virtual marketplaces and online shopping environment have added to the issue. In dealing with this data and information, security and confidentiality arise to be very important. In this thesis, we will consider issues like security and trust in IoT and local cloud interfaces and the security requirements of M2M services followed by suggested security solutions for internet based on their ineffectiveness.

### Motivation of research

The concept of web sessions is designed to authenticate the information of the users on the internet. Most of the web application uses these sessions to get the purpose. These

sessions limit the number of times; the users have to put their information in logging in the account. However, these web sessions are also vulnerable to the security concerns. OWASP, one of the most authentic organizations in the field of internet security, ranks these web sessions among top-level risks. This might be the reaction of vulnerabilities of attacks on the web session management of prominent web applications like YouTube and Twitter.

In this thesis, we will consider security and trust issues in IoT and local cloud interfaces. Along with the security, requirements of M2M services will be looked into. In addition, different architectures and protocols will be discussed in the perspective of the security phenomenon.

### Problem statement

The internet facilitates communication in the world. The issue of trust and security is increasingly important. When we want to understand human being, we learn their languages and communicate with them in their language. It is also the case with these systems and web applications, they also use certain forms of languages. The topologies,

protocols, and supplications in the system use language that needs to be run. In all of this discussion, our focus would be on security aspects. Security means the control over the access (Marlene and Maheu, 2005). The challenge in using local clouds is how to figure out these access controls by employing rights and roles between different clouds.

### Wireless Local Area Networks (WLANs)

A wireless LAN is the same as the wired LAN. The only difference is that transport medium in this regard is radio waves. In traditional wired structures, this medium is not used. This makes an environment under which the user can use the internet and keep connected with the world. However, the area it covers is of limited coverage (Corman, 2014). One of the benefits of WLANs is that it enables data connectivity with simpler structure with mobile features. WLANs are a solution to the web connectivity without wires that is its main edge.

The mobile devices are expected to increase, resulting in the increase in traffic of data. It is estimated that by 2017, the number of handheld and personal mobile devices would surpass the figure of 8.6 billion (economist.com, 2009). Along with this, 1.7 M2M connections will also be created. These M2M connections include GPS systems, asset tracking systems, and medical applications, among others.

The smartphone will continue to increase their market share. By 2017, they are expected to be 50% of the total market, declining the share of non-smartphones to 50% from 75% in 2012 (economist.com, 2011). The biggest growth is expected to be in the M2M and Smartphone. Average speed is also expected to increase many fold per device (Table 1).

M2M technology is supportive to wired and wireless communication. This technology is used in robotics, data collection, remote control, etc. The IoT in industries is witnessing rapid growth. The industries that are mostly benefiting from it include industrial automation industry, energy grid management among others. These wireless and M2M devices are renowned for their ability to collect and manage data and data traffic.

### Scope and limits of the study

Cryptographic protocols enable Wi-Fi to ensure privacy and security. For this purpose, WEP is the first cryptographic protocol to serve this purpose. Another cryptographic protocol, WPA was created by the Wi-Fi alliance to be consistent on security issues with WEP. WPA is considered to be secure despite offline dictionary attacks (Aihab Shehzadi, 2009). It is a good answer to the problems based on WEP. It is part of a Robust Security Network that was proposed by the Institute of Electrical and Electronics

**Table 1:** Summary of per device usage growth, MB per Month (businesswire.com, 2014).

| Device type    | 2012 | 2017 |
|----------------|------|------|
| Non smartphone | 6.8  | 31   |
| M2M module     | 64   | 330  |
| Smartphone     | 342  | 2660 |
| 4G Smartphone  | 1302 | 5114 |
| Tablet         | 820  | 5387 |
| Laptop         | 2503 | 5731 |

Engineers 802.11i in their draft. IEEE 802.11i is also covered in this thesis up to the extent of its similarities with WPA and RSN.

### LITERATURE REVIEW

Wi-Fi wireless web is User-friendly and accessible to a large number of companies and people but with the initiation of technologies it has become inexpensive. Different individuals in dense urban areas and access points are so closely belonging to their coverage areas spaced that overlap. This is the true story of the Bergen city shown in performance survey section (Cleland, 2011). Many individuals perceive Wi-Fi wireless as a hobby due to its accessibility and attractiveness to everyone. The Wi-Fi also kit into cars and in laptops by the war-drivers. The Global Positioning System (GPS) with the support of antenna and receiver become a good device to discover maps, areas and locations of important places. The purpose behind it is to develop vulnerable wireless networks and for the sake of fun. Same as the war-walkers and war-bikers do by using other sources of transportation.

### Wireless Local Area Networks (WLANs)

#### *Types of wireless networks*

According to the 802.11, Standard (Bagley, 2014), 1999 version there are three types of W-networks available for customers.

#### *Independent Basic Service Set (IBSS)*

The IBSS in general is known as an Ad Hoc Network. In the case of LAN network, it is comparable as Peer-to-Peer network shown in Figure 1. It communicates without any wired network and Access Point in IBSS having different end nodes (Michael Chui, 2008). Through this, network is set up quickly in no time in order to avoid unseen problems such as convention, publicly crowded areas and meetings.

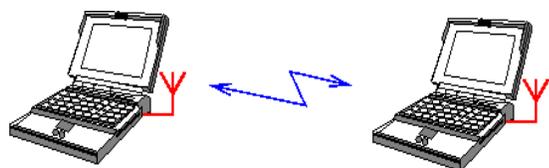


Figure 1: Ad-hoc mode.



Figure 2: Infrastructure mode.

### Basic Service Set (BSS)

It is an infrastructure Network having a single Access Point. It is the point through which all the communication passes by AP between two nodes. It covers a large area as compared with IBSS (Figure 2).

### Extended Service Set (ESS)

A Single Access Point having multiple BSSs is called ESS. In each ESS, an Ethernet Network is wired to the Access Point connected to a distribution system (Figure 3).

### Wireless Networking Standards

There are various WLAN standards, which are specified by the Institute of Electrical and Electronics Engineers (IEEE). According to requirement, some Standards are listed in Table 2.

#### IEEE 802.11b security features

These are provided in 802.11b standard (2).

#### Service Set Identifier (SSID)

It performs as WLAN identifier. All the devices are configured with SSID when trying to connect to a specific WLAN. A packet is sent over WLAN that is added to header, that is, BSS. It is also verified by Access Point (Russell and James, 2013). SSID is configured with the Access Point when the customer wants to communicate. Otherwise, he cannot have access.

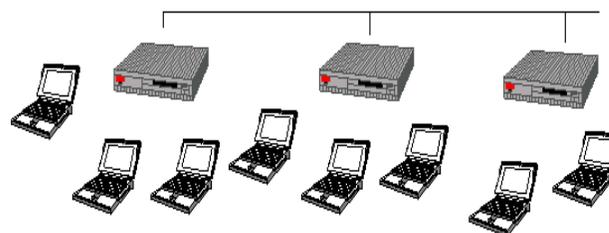


Figure 3: Extended Service Set (ESS).

Table 2: Wireless networking standards.

| Standard     | Description                                 | Approved  |
|--------------|---|---|
| IEEE 802.11  | Data rates up to 2MBPS in 2.4-GHz ISM band  | July 1997   |
| IEEE 802.11a | Data rates up to 5.4MBPS in 5-GHz UNII band | Sept 1999. End user products began shipping in early 2002 |
| IEEE 802.11b | Data rates up to 11MBPS in 2.4-GHz ISM band | Sept 1999. End user products began shipping in early 2000 |

### Wired equivalent privacy-WEP

It is associated with confidential wired local area network that does not occupy cryptographic techniques to increase privacy. The specifications for IEEE do not have encryption of data as required for Wired LANs. Controlled entrance and walled structures as physical means are secured by LANs. However, in case of WLANs, it has to clarify the need of encryption mechanism to provide physical boundaries (Carafano, 2012). The key is provided by WEP for symmetric Encryption. Each node is configured with this key manually. Encrypts is a sending station while decrypts is receiving station of the message using WEP key. The stream cipher RC4 is used by WEP.

### MAC address filters

It accepts the request of those nodes to be configured and registered them with the MAC to accept connectivity and relation requests with Access Point. An additional security layer is needed to provide for this scheme.

### Web server security challenges and defense

Security and privacy is a big issue in the present world. There are transfer and exchange of important data on the web therefore, the importance of security cannot be denied. There are a number of factors and individuals that create security problems.

**Secrecy**

It involves keeping data from unauthorized users. Security of the network refers to web security and secrecy. Only authorized parties are able to access information for reading in a computer system. The existence of an object, disclosure and printing are the simplest type of access given to authorized bodies.

**Authentication**

It is very essential to make secure the communication of data transfer between parties. Therefore, it is necessary to make sure that you familiar with the person to whom you are transferring data to. For this purpose, the authentication of person is needed.

**Non-repudiation**

The message contains signatures that deal with non-repudiation and unique characteristics of the person. For example, having mail via Hotmail using any signature.

**Integrity control**

After sending messages, it is necessary to know that the message sent is delivered to the right person and there is no modified transit adversary. It is a key to the authorized person to make changes in the computer system. The operations of modification are deleted, Update and Add. Four kinds of attacks that cause system interference are shown hereafter.

**-Interruption:** It destroys the system and makes the assets of computer unavailable to use. This includes bad sectors on hard drive, destruction in hardware, cutting supply to display and poor file management.

**-Interception:** The data are accessible to that person who is not authorized to use it. This attacks system secretly. Man and computer can be an unauthorized party. For example, illicit copying, programs, wiretapping to capture data.

**-Modification:** The attack on the integrity of data includes the tempering of data by an unauthorized party. The change in values, modifying the meaning of the message and altering programs is examples of modification.

**-Fabrication:** The file system, imitation objects inserted by an unauthorized party. However, it is said an attack on authenticity. The placing of false messages in addition to record file and network is an example of fabrication (Diana and Miraka, 2011). Abnormal behalf of the serve might be

due to malicious inputs and can flaws of attackers on the server. It is very hard to handle all such problems and inputs with care. For this purpose the validation inputs are performed in various ways.

**SQL injection and Brut-forcing**

SQL injection and Brut-forcing are some attacks from which the protection is essential. The following ways are used to secure a system.

**Client side validation**

The user script is validated with languages such as JavaScript and VBScript operating on the browser of the customer. The input can be controlled by putting a long address in XHTML:

```
<input type="text" name="username" size="30"
maxlength=10>
```

The limit of the input is property of the max length. For the purposes of simplifying the validation of processes, a dropdown is used to void malicious input menus as much as possible. It runs by the browser of the customer. Therefore, option of the script is off for the customer and process of validation may not work properly. The customer machine accesses the algorithm and validation script through client-side (Figure 4). It is not a wise decision to remain or trust only on the side of the customer.

**Database input validation-server side**

At the request of the customer, the pages are generated by Server pages. These pages are intelligent enough to respond on demand of the customer. Algorithms and server pages are hidden from the customer. However, input on the server-side is a good validation approach. The direct input is validated by the server programs on its side. These are ASP, JSP and PHP that transform information to Visual Basic, C+, Java, Served and DLL components that are rigid in nature (Crystal, 2011). The client and Server-side validation are the same in nature, having coding, and syntax programs are different. Therefore, it is estimated that the idea and concept of customer validation is understandable by reading. Here is a general model for Server Side Validation for easy to understand (Figure 5).

**Overlapping types of risk****Unauthorized remote**

Unauthorized remote users are able to make changes due to miss-configuration and Bugs problems on a Web server:

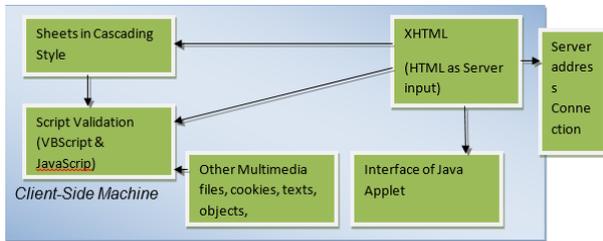


Figure 4: Client-side validation.

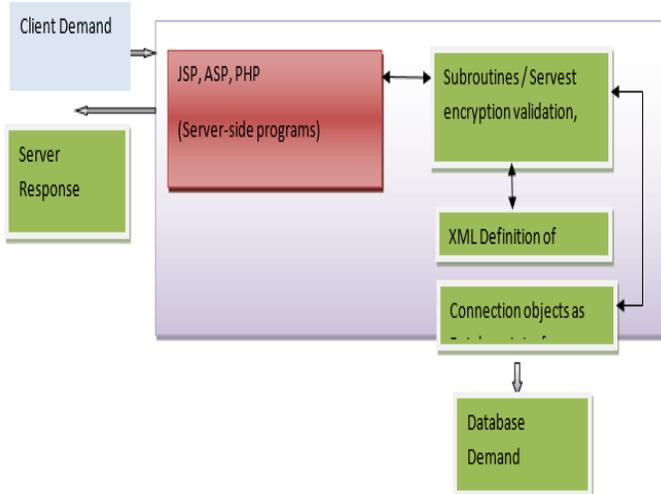


Figure 5: Database input validation-server side.

- A. Stealing of important and confidential documents
- B. Execute demand allows them to modify the system on the host server machine
- C. The system is broken by them because they have hosted machine Web Server's information
- D. The machine is temporarily unusable due to render by denial-of-service- attacks launch against it

**The risk of browser-side**

- A. The browser is crushed by active content and damages system, violates the privacy policy and also creates aggravation to users
- B. The unethical use of information provided by the final-user

**Network eavesdropping**

Network eavesdropping is sent from the browser to the server by interception of network data. The pathway between server and browser can operate through eavesdroppers. This includes:

- A. Connection on the browsers side network

- B. Connects to the server-side of the network
- C. Internet service provider to final customer/user
- d. ISP server

For the protection of confidential data and information opposing network, eavesdropping are only developed for servers and the browser's security. It is very important to realize the importance of privacy and security (Robert and Thierauf, 2013). Server-side, database server, browser and confidential information are susceptible to interception without the security of a system.

**SQL injection: A common threat**

It inserts the SQL statement without permission of the side server programs to run the database. When users input its name, this injection occurs to ask a logical name and SQL statement in order to gain access, steal information by running database directly (Geron, 2013). For example, to bad and normal user, SQL Injection is trying. The user is asked for his/her login name to get information that will be used to run a SELECT statement.

**Description**

The SQL statement will select username equal to the string Peru from customers. This little query is not a big problem. The estimation about the attack of SQL injection makes different behavior of our query. The string part of our query is by using single quotes ('). They have ended other malicious query quote (') after the string of SQL.

```
Username ="
WHERE statement is then added with an OR clause of 1=1 is always true.
Username = " OR 1=1—
```

Therefore, the single entry in client table would be selected by this OR clause of 1 and displayed by statement will always true. Due to underestimate of this injection, the company has to suffer with huge losses, and attacks may be worse more as expected. This attack can delete the database results (Figure 6).

**Defeating the SQL**

- (1) To filter the dab string, write DLL or Servlet in server-side function
- (2) With `MYSQL_REAL_ESCAPE_STRING ()`

To prevent the attacks of these known problems, a specially-made function of the PHP is used. That is, the function `mysql_real_escape_string` is used for these problems. The string that is to be used in the MySQL query

```

MYSQL & PHP Code:
-----
$name_evil = "";
DELETE FROM customers WHERE 1=1 or username = "";

// our MySQL query builder really should check for injection
$query_evil = "SELECT * FROM customers WHERE username = '$name_evil'";

// the new evil injection query would include a DELETE statement
echo "Injection: " . $query_evil;
-----
Display:
SELECT * FROM customers WHERE username= ''; DELETE FROM customers
WHERE 1 OR username='';
-----
It results to completely empty the "customers" table in the database.
    
```

Figure 6: Example of injection.

is taken by the function and return same string, with the SQL injection attempts to escape safely. The basic troublesome quotes(') will replace and enter with safe substitute MySQL. The quote /' is an escaped function. How these injections work and attacks are shown hereafter.

**Brut force defense with human / program recognition (CAPTCHA)**

It is commonly observed that when there is an attempt to unsecure or unsuccessful login, the server verifies the identity with verification codes, which are a combination of alphabets and digits. These randomly generated images of this combination are hard for Bruit-fruit to recognize the software (Isaac and Porche, 2013). The brut-fruit use relevant dictionary to login user name and password with automated attempt. Most of the time, this method is done with the support of computer software.

The messengers and search engines like Hotmail, Yahoo mail and Gmail are using that combination of digits and alphabets as verification codes in order to enhance the security of the clients. This will help software to identify that login attempt is by automated software or human. The system of generating these combinations to form verification codes is called Captcha system.

The automated login-request has some predefine attributes generated by computer software as time passes between login attempts more than one. There will also be numerous attempts of login having a specific time interval between each attempt. In case of human attempts, there is no such functionality. This is helpful for the system easily recognize that request for login is made by human. This will also distinguish requests generated by software and human with the concept of Captcha (Figure 7). Client-Side also requests for filtering rapidly up to a level, whereas this system is also implemented in Server Side.

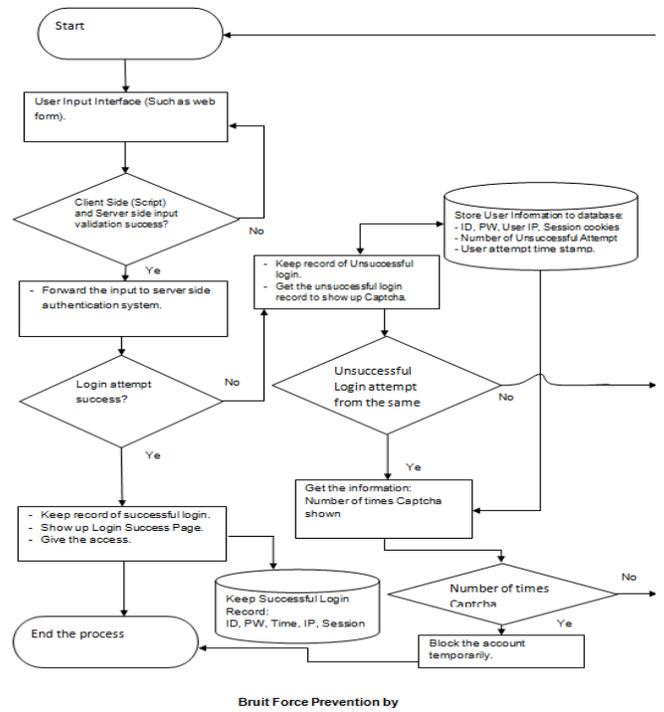


Figure 7: The Flowchart shows the basic functioning of Captcha.

**Disaster recovery plan**

In this age of information, the businesses have web services as the integrated part. The web services may be disturbed due to unforeseen disasters that cause business to down. The loss may be in terms of revenue, reputation, money and profit, which drives business towards failure. The Disaster Recovery Plan (DRP) is set to survive from IT-Disabling disasters (Kabat, 2014). DRP is designed to continue the procedures and policies of business without any interruption and loss. Therefore, the core and central components of business and web services run smoothly with help of Disaster Recovery Plan (Geoffrey and Greif, 2005). It is well stated, "Dollars spent in prevention is worth more than dollars spent in recovery".

**Risk analysis**

This is done to establish all the risks that interface a system. Before drafting DRP, a risk analysis is very crucial at the first stage. The server is unavailable and out of order due to some common reasons stated as:

- Datacenter request for flood
- Blacked-out or electric power shortage on server
- By uploading of unexpected malicious, server software crash
- Threat of server hacking
- Hardware and physical breakdown or failure of server

- Maintenance of server on regular bases
- Natural disasters like fire, storm and earthquake

It is necessary to have some meetings and brainstorming to find all the possible threats and risks of server failure and its prevention in IT department. The risks can be ranked on the basis of occurrence probability and its influence.

### ***Budgeting and feasibility study***

The second step at DRP is the budgeting of finance strategically and wisely. Numbers of solutions are determined for a single problem in order to ensure that the solution's quality is good enough to communicate cost and become a unique best solution for that problem (Ramessur, 2013). The process of generating and selecting a high quality solution is called Feasibility study.

### ***Develop and implement the plan***

IT department should write down all the recovery and procedure script details. All other departments and units also take part in decision-making and give their suggestions to the IT department for the implementation of DRP. The IT department receives feedback from various units in an organization (Radack, 2014). For example, the DRP team responds to any suggestion given by another department as well. If another department points out that 46 hours are viable for the incident to be recovered, then the team calculates the time and other factors to make sure that this idea is either effected or not. They also established the backup plan for business in the given time frame to solve the issues regarding operations (economist.com, 2014). The recovery plan and services might be backup for business.

**-Testing:** The final stage after the DRP is set up in a company is the testing of the system. It is observed through experimentation that how the system works in possible disaster and consequences. The system is tested for all problems and issues to make sure the validity of DRP.

## **ALTERNATE SOLUTIONS TO MANAGE THE WIRELESS WEB SECURITY SERVICES**

### **IEEE 802.1x**

This is the authenticated port-based protocol, which includes various three types of the protocols. IEEE 802.1x is classified into categories and offers the respective detail of those sufficient entities that shall maximize the outcome of surfer with the internet protocol. This type of the network has always included a server, a supplier, an authenticator, a supplicant and a person who manages the resources

through the internet-based services. This is mostly used with the 802.11b LAN and the 802.1X which consist of the following significant features:

### ***Logical ports***

These are the ports which the internet is connected. These ports are connected through the wired and the wireless stations. These stations ultimately decide the relationship between the sources of the internet and reflect the presentation on the internet related aspects. To survive accurately through the internet sources and manage the data, the WLAN connection is meant through the logical ports. A logical port is usually established through the connection between the wired and the wireless stations (Maarten, 2013). There are a number of access points, which are connected logically to establish the connection. Any division or disturbance in the ports shall ultimately result in the insecurity of the internet devices. The division of the internet devices is respectively managed through the wireless work stations. Hence, this station works effectively through the EAPOL protocol exchanges. The EAPOL ports send the messages through the r IEEE 802.1, considering it as the basic link of the ports (Figure 8).

### **Key management**

IEEE 802.1x is the main WEP key which is widely used for the encryption of data aimed at the internet. It passes the information over the wireless sources of the internet and prefers the respective details of the EAPOL-key. This key is considered as the best source of offering the information and the respective details of the wireless data on the internet. The information is authenticated by the internet supplier on the web and the supplier offers the respective aspects of the management of the data. It deals with the management of the financial and the non-financial aspect of the internet managements, which prefers to deal the managerial source foe the internet. The Expel is managed through the internet supplies those are Carrie dander the authenticated message of the Supplicant. The EAPOL shall reflect the respective internet sources that shall associate with the wireless and the wired internet. As well, they shall offer the details about the presentation of the server errors and the authenticated details about the data presented. Figure 9 shows the details of the relationship between supplier applicant and the server in the network.

### **VIRTUAL PRIVATE NETWORK (VPN)**

A VPN is the source of the wireless internet that offers the data through the secure medium. It manages the data sources through the internet, sources of data. This offers

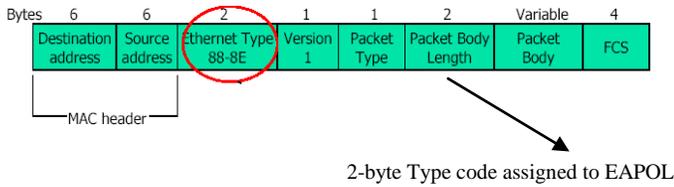


Figure 8: EAPOL frame format.

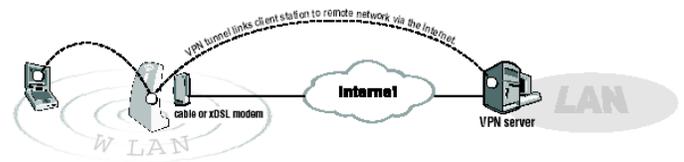


Figure 10: Access Point with VPN.

Supplicant Authenticator Authentication Server

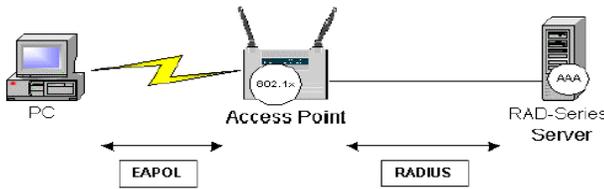


Figure 9: IEEE 802.1x in 802.11 WLANs.

the medium to support the internet supplies and offer the required amount of information through the secured measures (Lyon, 2013). The virtual networking is another modern technique used by the modern day people to support the wireless secure network.

Overview of VPN

The VPN networks are generated on a tunnel, which satisfied the requirement of the internet. The tunnel is supposed to offer the required details, information and the details for the wireless internet sources. This tunnel offers a wide variety of information that is secure and scanned through the three respective sources of the wireless LAN configuration (Figure 10).

- Authentication
- Encryption
- Data authentication

Testbed setup

Desktop computers

The desktop computers use the categories of the Intel based desktop computers. Both of them are associated with the accessing points of the infrastructure-based WLAN. Therefore, the accessing points of the infrastructure-based WLAN provide the various configurations of the desktop computers.

Hardware configuration

The hardware configuration includes the process chip, RAM and the network adaptor that provide the big picture related to the different series of the wireless LAN adaptor that makes enable to all wireless systems and improve the importance of effective connectivity between the client and the server.

Software configuration

The software configuration includes the operating system that enable to the running system that support all activities.

**Experimentation-** To resolve the WEP susceptibility, there are four various solutions provided. These include IEEE 802.1x, which stands on EAP, and Cisco LEAP. These two solutions will be treated for the purpose of assessment and examination of the vulnerability issue. Since both are of the same techniques, so we will use only the Cisco-based joint analysis of our cases. For the purpose of demonstration and convenient implementation, we will use a prototype of WEP. By doing this, we will check the susceptibleness of the WEP issue. Different testing techniques and procedure for experimentation are given hereafter.

- Legends

- Denote safety management;
- \_\_\_\_\_ denotes data course
- SP Denotes Java program that fetches data between client and server.

-WEP supported technique

To secure the WEP configuration, the WEP key will be physically settled to ensure WEP safety. SP act as produce example information as shown in Figure 11.

-Leap supported technique

In this technique, client laptop will serve as LEAP supported as shown in Figure 12.

-LEAP-enabled Set-up

This technique will make the desktop as a RADIUS server.

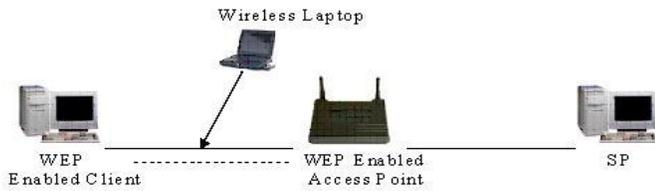


Figure 11: WEP-enabled set-up.



Figure 12: 2 Leap supported technique.

**VPN supported technique:** This technique will use the VPN awareness system, which means that desktop computer, will be settled with VPN and it will act as VPN junction. Beside this, there would be an option of the AAA serve. This will be done by installing VPN software in a desktop computer. This can be seen in Figure 13.

### WEP privacy breakdown

WEP privacy is enabled by designing procedures to lock all the data used in the function. However, a hacker can get access to the system by breaking passwords through 7 ways.

These ways are:

1. By intruding into the algorithm and breaking it to get the key. This is due to the flaw of RC4 algorithm.
2. Another way is by hitting the key in the sudden vocabulary assault.
3. Unlock the system network by using the database key sequence. It can be possible if the sequence pattern of data base keywords is already known.
4. This protocol can be a breakdown by intruding into the hopeful texts' guesses.
5. Where locks are present in double sequences, then it means it is almost unlocked.
6. A hacker can send some sort of information package, which is sent to the IP controller, when the controller respond to it, then it unlocks the network security.
7. In some cases, the hackers try to input some most used keys for the purpose of encryption, to decrypt the network.

There are some cases, which will, only be useful in specific circumstances, like the cases 2 and 4. Meanwhile case 3 is a



Figure 13: VPN supported technique.

tough job because it needs a specific large amount of disk space and some additional time. The biggest threat to the WEP failure is that the hacker is able to get through the key to the network. As soon as he intrudes into the system information to get WEP key, then it is certainly the biggest failure of the WEP (Konrad, 2013). To do this, hacker just needs to get to the signals of the Wi-Fi, software that are open resource and radio devices.

To reconcile the attack, the first way is to end the flaws in the algorithm. There is also a mechanism to finding the secret key by finding the one by one-secret weak keys. Hacker does this type of things and RC4 itself expose the secret key (businesswire.com, 2014). Once the first key of encryption is identified, the hackers' system automatically generates all the possible sequence of the keys.

Similar way is by catching an oral expression. It is captured in steps as follows:

1. Catching an encryption phrase
2. Then take out the first 2 and 4th byte of the flow of keys.
3. When the 4th is not beneficial, it is meant to say when it does not give information about the RC4 weak key, then hacker can pay no attention to it.
4. The information, which you have collected until now, finds a possible key value.
5. If still not done, then revise the whole steps from one to now, until the information is regained.

When the information collected provide you sufficient enough that give you keys, then analyze it time by time. In some circumstances, it needs sufficient time to complete the process because to get through IV is time consuming. In this section, it is demonstrated that if the mechanism of "IV acceleration" is adopted, then it reduces the procedure time by half. It means when a hacker is not using "IV acceleration", then it will take two hours, but when he is using then it will take an hour.

### Wi-Fi PROTECTED ACCESS (WPA)

Wi-Fi protected access gives the short explanation of how the user can protect access of the Wi-Fi system through the security mechanism. Wi-Fi Protected Access can be demonstrated with the common modes of security process related to the Wi-Fi protected access. There are two processes that explain the actual meaning of the user

security. The first is the background and the second is WPA-PSK, both are working on the protected access of the wireless system (Plante, 2014). Wi-Fi protected access is the common mode of planning related to the pre shared key indicator that provide a key to the user, which help to protect all the data. Pre-shared key is the secret key which have the importance in the client networking because it provide a secure number of sharing network and this number is limited to those people who know about the security password of the wireless system.

### **Breaking confidentiality of the access point**

Wireless breaking confidentiality can be broken with the help of WPA. Because if any person knows about the Wi-Fi protected access, then you can find the way to do all the things in an efficient and effective way. WPA key is also generated with the help of Passphrase. Through the four different ways we can identify the wireless protective key that will help in the security of the data.

### ***Recovering a passphrase seeded WPA key***

Wi-Fi protected access point cracker is the first tool that helps to implement an attack of an offline dictionary against the WPA. The performance of this cracker is approximately equal to the 24 passphrase per second. This tool of WPA cracker requires the tool of nonces and SSID that help to measure the security performance as well as it can be manually inserted at the time of window startup.

At the time selection of the passwords, some people use the correct password and choice the QWERTY tabs and used the numbering as well as capital letters that help to strong the passwords and makes them more protected. Sometime people do not choose the right options for the selection of the password, that is why it is not working properly and the strength limit is weak, which can be easily accessed by others. If the strength limit is weak, then the Wi-Fi Protected Access router configuration is very easy to find out by browsing and hacking the passwords of other routers. Users do not use the important passwords at the time of router configuration and choice the simple passwords for the initial stage of the Wi-Fi Protected Access router configuration.

### ***Packet injection***

In the Wi-Fi protected access point, we can choose the packet injection that is working for the arbitrary type of data as well as restore all the data according to the proper timing and date of the install data. The method of breaking confidentiality is becoming the result of the exposed key sequences of the normal word lists. A key sequence can be recovered through the client authentication mechanisms

that help to recover all the work in an efficient and effective way. In the packet injection, there is no rule of the sequence numbering and no rule on the values of the injection of the packet data. Key sequences can be used for many times and do not select the values related to the numbering of the given data. Key sequences can be used since the time of adding value as well as it can be used at the time of making the pairs of matching numbers.

**IV Acceleration:** IV acceleration is the process of the collection that helps to increase the cipher text pairs. IV Acceleration plays an important role in cracking the key elements of the WEP. Wi-Fi protected access points is used as tricked that transmit all the data related to the encrypted frame of work. IV Acceleration is the new mode of collection of the data. For the accomplishment of all the tasks the attackers related to the inject packets needed as well as many options of the retransmit. The tool of retransmit plays an important role to capture the packets as well as increase the number of the receiving the new replies. The other approach of the IV Acceleration is the Transmit de-authentication frames that deal with the clients and provide re-authentication in case of transmission of the data.

**Retransmission:** Retransmission is the technical tool that helps to use the air crack, which only needs proper monitoring under the required software. Retransmission is trying to force the re-authentication that improves the slow process that compares the different options of the key sequences as well as the normal list of wording.

The Retransmission as well as packet injection needs the proper transmission of the data and the additional knowledge on how to solve all the things in an efficient and effective way. In the Retransmission process, it does not only need the improved knowledge, but also record the IP address that helps to connect with the Wi-Fi Protected Access Points (Bagley, 2014). IP address helps to deal with all things related to the security of the Wi-Fi Protected Access as well as Wi-Fi router configuration. Air crack performs their function as a wireless and do not more wires for the connectivity. Technology change day by day, therefore, information technology professional and operators need the up-to-date knowledge to update their knowledge according to the new techniques and provide the new services of the connectivity. If the knowledge is not required at, the due time, then skipped those sections.

### **MAC address**

The MAC address is another tool of the systemized network which includes the traffic of the empty network. The empty network identifies the access points of Wi-Fi Protectiveness. Thus those frames that come from the side of authenticating clients are accepted only. If the clients are not connected to the empty network, then those frames of

work are not included in the process of the empty network. The empty network plays an important role in the authentication process.

The authentication mode of the network is an open network that is associated with the ARP packets and broadcast address. The MAC address is also called the board, cast address that has come under rescue and provide the number of clients on the wired network. The empty network induces the different traffic related to the transmission (Figure 14).

### Time needed to gather enough IVs.

Diagrams need the together IVs that help to connect all the data and improve the level of the recover data. In the IV acceleration, the measured required data play an important role in increasing frames of per second transmitted network. The transmitted network operates with the different rates of the IV acceleration and enables the recovery of the lost data.

When the WEP key performs its activities in the fastest way, then it becomes easy to recover the data with the help of the VI acceleration. It has been determined how frames perform their tasks according to the various transmissions (Bernadette, 2014). Various rates of the operating system help to evaluate the results of the benchmarking programs.

### Security supplements

In the security, supplements included the different number of addresses and the filters that play an important role in the bypass of the MAC address after filtering the points of the optional security mechanism. The number of the security supplements helps to specialize the number of the different:

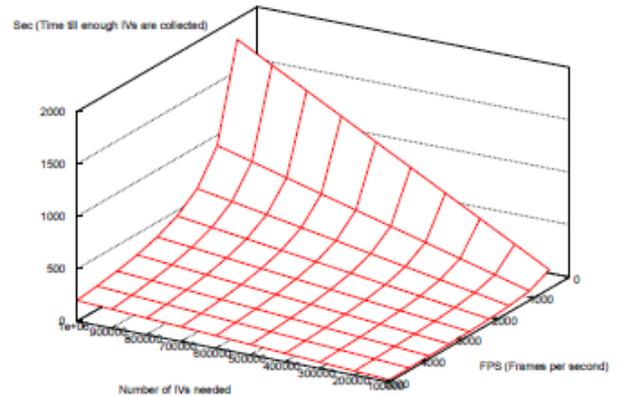
- Bypassing MAC Address Filters
- Avoiding Interference
- Defeating Captive Portals

#### *Bypassing MAC address filters*

MAC address filters are found in the different Wi-Fi assessing points that play an important role in the optional security system. The purpose of the MAC address is to deny the access of the networking interface.

#### *Avoiding interference*

If the two computers are connected with each other, one connected to the clients and other one the intruder, then



**Figure 14:** Results of the inducing traffic related to the empty network.

the communication of both computers will be disturbed, and therefore, creates interruption between all the data (Bendary, 2013). So, at the time of sharing the data, client and intruder must be avoided to prevent interference between the computers.

### CONCLUSION

Conclusively, websites play an important role in promoting business through social media by publishing the different blogs and articles that improve the level of information on how businesses are working and what functions are performed under this business. The up-to-date knowledge about the business activities promotes business with the help blog and articles writing. Thereafter, it provides facilities to the customers related to the online shopping and easy modes of the financial transactions which promote the value of the business. The security programs related to the Wi-Fi networks play an important role on how to cover the distance and connect the network to the personal computer. When two computers are sharing information with each other, there are many less chances that they are effective because they need to be proper system that individually performed. If using computer with the direct interference, then the user and clients are both disturbed because they are not able to effectively communicate it due to repeated disconnection of the data.

### RECOMMENDATION

The devices that are used to identify malfunction over the internet are called intelligent devices. These intelligent devices have been much innovative in the last few years. The advantages of these devices are clear as they enhance productivity, efficiency in decision-making process. One

problem has been associated with these devices, that is, lack of integration. These technologies embrace innovations and improvements taking place in other fields, but after completing their product, they work in isolation. The features these devices provide do not decrease, however, lack of integration is a problem in its place.

Machine to machine applications are used in businesses to be reliable and trustworthy during the operations. Using these applications, data are sent to remote centers of application and data stores for further processing. The problem with this approach is centralization that invites heavy flow of traffic. In contrast, decentralized networks have come into being, that allows storing data close to the devices, rather to be sent to remote applications centers. Then, before sending the data over the internet, it is aggregated. These decentralized networks are also called local clouds. These clouds were the very effective solution to overcome the high traffic on mobile networks.

## ACKNOWLEDGEMENTS

The author would like to express special thanks to his thesis advisor, Dr. David Anyiwo, for his precious suggestion and encouragement. Also, special thanks to his professors, parents, and friends for their encouragement and inspiration to the thesis, related study and research work.

## REFERENCES

- Aihab Shehzadi E (2009). SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security. *Issues in Informing Science & Information Technology*, 1-12. Retrieved 6 17, 2014, from [Issues in Informing Science & Information Technology](#).
- Bagley RO (2014). How The Cloud And Big Data Are Changing Small Business. Retrieved 6 18, 2014, from <http://www.forbes.com/sites/rebeccabagley/2014/07/15/how-the-cloud-and-big-data-are-changing-small-business/>.
- Bendary N (2013). Intelligent Detection and Control for Environmental Noise Pollution. *Am. Acad. Scholarly Res. J.* 5(3):1-9.
- Bernadette W (2014). Managed Services, Backup and Recovery, and Networking News From June 2014. Retrieved 6 17, 2014, from <http://www.bsminfo.com/doc/managed-services-backup-and-recovery-and-networking-news-from-june-0001>.
- businesswire.com. (2014). elit Expands m2mAIR Mobile Coverage Across Europe and Latin America in Partnership with Telefonica. Retrieved 6 18, 2014, from <http://www.businesswire.com/news/home/20140717005161/en/Telit-Expands-m2mAIR-Mobile-Coverage-Europe-Latin#.U8jIEJSSxvQ>
- Carafano JJ (2012). *Wiki at War: Conflict in a Socially Networked World*. Texas A&M University Press.
- Cleland S (2011). The Next Leg of Wireless Growth? Retrieved 6 18, 2014, from <http://www.forbes.com/sites/scottcleland/2011/10/11/the-next-leg-of-wireless-growth/>
- Corman (2014). Home, hacked home. Retrieved 6 17, 2014, from <http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home>.
- Crystal D (2011). *Language and the Internet*. Cambridge University Press.
- Diana L, Miraka JB (2011). *The Power of Convergence: Linking Business Strategies and Technology Decisions to Create Sustainable Success*. American Management Association.
- economist.com (2009). In-flight internet is it secure. Retrieved 6 18, 2014, from [http://www.economist.com/blogs/gulliver/2009/05/inflight\\_internet\\_is\\_it\\_secure](http://www.economist.com/blogs/gulliver/2009/05/inflight_internet_is_it_secure).
- economist.com (2011). Worrying about wireless. Retrieved 6 18, 2014, from <http://www.economist.com/node/21527022>
- economist.com. (2014). Defending the digital frontier. Retrieved 6 18, 2014, from <http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals>.
- Geoffrey L, Greif PH (2005). *Group Work with Populations at Risk*. Oxford University Press.
- Geron T (2013). Data For Nothing, Calls For Free: How FreedomPop Will Offer Free Phone Service. Retrieved 6 18, 2014, from <http://www.forbes.com/sites/tomiogeron/2013/06/05/data-for-nothing-calls-for-free-how-freedompop-will-offer-free-phone-service/>
- Isaac R, Porche IP (2013). *Redefining Information Warfare Boundaries for An Army in a Wireless World*. rand.
- Kabat G (2014). Do Cell Phones Cause Brain Cancer? The Diehards Cling Desperately To Opinion. Retrieved 6 18, 2014, from <http://www.forbes.com/sites/geoffreykabat/2013/03/05/do-cell-phones-cause-brain-cancer-the-diehards-cling-desperately-to-opinion/>
- Konrad A (2013). Tesla Now Connects Every Car To Internet Through AT&T Wireless, But It's Not 4G LTE. Retrieved 6 18, 2014, from <http://www.forbes.com/sites/alexkonrad/2013/10/17/tesla-att-connected-cars/>
- Lyon D (2013). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Routledge.
- Maarten BRH (2013). *Enabling the Information Society by Stimulating the Creation of a Broadband Environment in Europe: Analyses of Evolution Scenarios for Future Networking Technologies and Networks in Europe*. Rand.
- Marlene M, Maheu ML (2005). *The Mental Health Professional and the New Technologies: A Handbook for Practice Today*. Lawrence Erlbaum Associates.
- Michael Chui ML (2008). *The Internet of Things*. Retrieved 6 18, 2014, from [http://www.mckinsey.com/insights/high\\_tech\\_telecoms\\_internet/the\\_internet\\_of\\_things](http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things).
- Paton J (2014). Bechtel-Union Discord Raises Australian LNG Plant Delay Risk. Retrieved 6 18, 2014, from [http://www.bloomberg.com/news/2014-07-18/bechtel-union-discord-raises-australian-lng-projects-delay-risk.html?cmpid=msnmoney&industry=IND\\_ENERGY&isub=Plante](http://www.bloomberg.com/news/2014-07-18/bechtel-union-discord-raises-australian-lng-projects-delay-risk.html?cmpid=msnmoney&industry=IND_ENERGY&isub=Plante)
- Plante A (2014). On Point: Cloud Advancements and Encryption, Web Security Updates. Retrieved 6 17, 2014, from <http://channelnomics.com/2014/06/20/point-cloud-advancements-encryption-web-security-updates/#.U8eM5pSSxvQ>.
- Radack S (2014). SECURITY FOR WIRELESS NETWORKS AND DEVICES. Retrieved 6 18, 2014, from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>.
- Ramessur RT (2013). Computer-Mediated Communication for Effective Teaching-Learning of Coastal Zone Management Module. *Int. J. Educ. Dev. Inform. Commun. Technol.* 3(1):1- 4.
- Robert J, Thierauf J (2013). *Smart Business Systems for the Optimized Organization*. Praeger.
- Russell G, James L (2013). *Cloud Computing for Small Business: Criminal and Security Threats and Prevention Measures*. *Trends Issues Crime Crim. Justice* 456(1):12-18.