Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology

Bachelor Thesis

Wireless LAN Security

Miah Md Rasel

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Md Rasel Miah

Systems Engineering and Informatics
Informatics

Thesis title

Wireless LAN Network Security

Objectives of thesis

To find out different sides of Wireless Local Area Network(WLAN) security and to illustrate possible attracts on a secured network. To study present WLAN security and potential issues associate with security. To do an experiment to break a secured network by WEP and WPA and to describe a possible solution for improving WLAN security.

Methodology

The method will be the Deductive method. The main method of the research will be the comparison of different security features and performance, characteristics of some security technologies. There will be encryption and authentication methods, for example, WEP, WPA, WPA2, WPA3 to differentiate theoretically.

The proposed extent of the thesis

40

Keywords

Wireless Network,network security,Network attracts,WEP,WAP

Recommended information sources

B. P. Crow, I. Widjaja, J. G. Kim, & P. T. Sakai, sIEEE 802.11 Wireless Local Area Networkss. IEEE Communication Mag., vol. 35, no. 9, pp. 116-126, Sep. 1997

https://www.infosec.gov.hk/english/technical/files/wireless.pdf

Expected date of thesis defence

2020/21 SS – FEM

The Bachelor Thesis Supervisor

Ing. Tomáš Vokoun

Supervising department

Department of Information Technologies

Electronic approval: 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 09. 03. 2021

Declaration

I declare that I have worked on my bachelor thesis titled "Wireless LAN Security: The Role of Intrusion Detection System" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 15.03.2021 _____

Acknowledgement

I would like to thank Professor Ing . Tomas Vokoun for his advice, support during my work on this thesis.

Wireless LAN Security

Abstract

In this research, we discuss about the wireless LAN and network security. Truly speaking, the present world is the digital world and we cannot deny the and live without wireless networks. Reality is that, in present era, humans become machines due to internet access and digitalization. Humans are facilitating everywhere where they live, they work, they spent precious moments of life. Their lives become more comfortable and even dependable on internet. In this study, we also analyze the security issues and even vulnerabilities in wireless network security with threats and dangerous in networking. We put light on different types of wireless security networks and recommendations. Furthermore, in this study we also shed light on evolution of wireless network and local area network.

Keywords: LAN, Network, Security, WEP, WPA, Internet, Intrusion, Digitalization, wi-fi, SSID

Zabezpečení bezdrátové sítě LAN

Abstrakt

V tomto výzkumu diskutujeme o zabezpečení bezdrátové sítě LAN a sítě. Skutečně řečeno, současný svět je digitální svět a nemůžeme popřít a žít bez bezdrátových sítí. Skutečností je, že v současné době se lidé stávají stroji díky přístupu k internetu a digitalizaci. Lidé usnadňují všude tam, kde žijí, pracují, trávili vzácné okamžiky života. Jejich životy se stávají pohodlnějšími, a dokonce spolehlivými na internetu. V této studii také analyzujeme bezpečnostní problémy, a dokonce i zranitelnosti v zabezpečení bezdrátové sítě s hrozbami a nebezpečnými v sítích. Osvětlujeme různé typy bezdrátových bezpečnostních sítí a doporučení. Dále v této studii vysypali světlo na vývoj bezdrátové sítě a místní sítě.

Klíčová slova: LAN, Síť, Zabezpečení, WEP, WPA, Internet, Vniknutí, Digitalizace, Wi-Fi, SSID

Abbreviations

WLAN	**Wireless Local Area Network**
WEP	**Wired Equivalent Privacy**
WPA	**Wi-Fi Protected Access**
PAN	**Personal Area Network**
PPTP	**Point To Point Tunneling Protocol**
PIN	**Personal Identification Number**
EAP	**Extensible Authentication Protocol**
DES	**Data Encryption Standard**
EMW	**Electromagnetic Waves**
BSS	**Basic Service Set**
SSID	**Service Set Identifier**
GPS	**Global Positioning System**
GPRS	**General Packet Radio System**
HTML	**Hyper Text Markup Language**
IP	**Internet Protocol**
I&A	**Identification and Authentication**
GMS	**Global System for Mobile Communication**
ISS	**Internet Service System**

List of Figures

List of Pictures

List of Tables

Contents

1 Introduction

We are living in the world of science and technology. Technology has been an amazing part of our life from a very long time since the birth of the Internet and networking. Since then, it is being updated modified and now we can see the affordability, the benefits and the easy use of internet in also every aspects of our life. One of them the Wireless networking. Through the implementation of wireless network, we made our purposes even easier and comfortable. Before the invention wireless network, we had to use cable-based network everywhere and which was expensive, time consuming and not easy task to manage everything. Implementation of wireless network in LAN is not very difficult task also its not expensive. Besides, the access of using it much easier than the cable based one. The big problem of wireless network is attracted from the hackers. Nowadays, hackers and cyber attracts is a very big matter of concern of this Internet world. Hackers can get to this network easily if the advanced and secured technology is not used for the implementation of the networking. Attacks can be active and passive, so the security of the network is a very challenging task to secure the data and the assets of the organization.

2 Objectives and Methodology

2.1 Objectives

To find out different sides of Wireless Local Area Network (WLAN) security and to illustrate possible attacks on a secured network. To study present WLAN security and potential issues associate with security. To do an experiment to break a secured network by WEP and WPA and to describe a possible solution for improving WLAN security.

2.2 Methodology

The method will be applied in a deductive way and as the main research method, there will be used the comparison of different security features and performance, characteristics of security technologies. Later, there will be used the encryption and authentication methods, for example, WEP, WPA, WPA2 and WPA3 to differentiate the research theoretically.

2.2.1 Research approach

The research approach is defined as the planning and the research procedure which is to be used for data collection, analysis, and interpretation of the research data [1]. The overall decision involves which approach should be used to study a topic. It includes assumptions about the details of the research analysis.

The research approach is divided into two categories:

- **Data Collection**

Data collection refers to the complete procedure of collection and analysis of the data samples. Data collection is further subdivided into two parts:

- Qualitative Approach: This type of research is expressed in words. It is said to be a detailed in-depth study and research on the topic [2]. No numbers or numeric values are used in the qualitative approach of data.

- Quantitative Approach: This type of approach involves the representation of research data in numbers, numeric values, and graphs. It is the statistical study type of research.

In this research work, both qualitative and quantitative methods of data approach are used to understand encryption and authentication operations of WPA, WPA2, WPA3 and WEP.

- ***Data Analysis***

Data analysis is one of the most crucial steps of the research approach. It helps minimize large data size to smaller parts which become easier to interpret. Data analysis is further subdivided into two parts-

- Inductive**:** Indicative data analysis helps in deriving concepts from raw data with the help of a research evaluator.
- Deductive**:** Deductive data analysis refers to developing theory and hypothesis and analyses the data to test the hypotheses.

In this dissertation, as per the deductive approach, there will be used the comparison of different security features and performance, characteristics of security technologies.

2.2.2 Research design

The research design refers to the overall steps and procedures undertaken to carry out the research work. Research design helps in identifying and reviewing the problems faced during the research work, describe the data collected for the research work, describe the research analysis method in determining whether the hypotheses are true or false [3]. A proper research design helps in a successful and unbiased research result. Research design has certain characteristics, as follows:

- ***Reliability:*** The research design should be reliable and should provide the expected results.
- ***Generalization:*** The research design should be such that it will be applicable anywhere. Hence, a generalized design is always preferred. [4]

- ***Validity:*** Multiple tools are used in measuring the research results and only after that, the research work is considered valid.
- ***Neutrality:*** The results of the research should always be neutral and unbiased.

Research design can be depicted in graphical or numerical form or in a detailed explanatory form. Both ways work fine as long as the research gives an unbiased result. The research design is the pillar of any research work. The research design determines which tools are to be used in the research work and how. Research design can be classified into four types:

- Correlational
- Experimental Research
- Descriptive
- Causal-Comparative/Quasi-Experimental

3 Literature Review

3.1 Wireless security

A network is consisting of two of more computers in order to share resources and allow electronic communications according to FCIT agency (2016).

LAN or Local Area Network is such a network which is generally confined for a small area, for example, University campus, school, building and small offices or restaurant and cafeteria. In the part, LAN network was used with cable connection but after the invention of Wireless technology, it is being used without using cable but the radio frequency.

A wireless network is a network which allows devices to stay connected to the network but roam release to any wires. Access points amplify WI-FI signals, so a device can be far from a router but still be connected to the network. For example, when we connect to a WI-FI hotspot an airport or a hotel or restaurant, we are connecting to wireless network as it was stated by Cisco [5].

In the beginning it was thought that, it is better to use cable based network because of its speed and security but as time goes and new technology was invented and the advance security features, Nowadays, we can see the widespread use of wireless network in school, colleges, universities, restaurants, cafeteria, small offices, at home and airport etc.

We can separate the background literature into three categories for examples:

1. Basic security of WLANs
2. IEEE standard
3. Detect or attack of WLANs

3.2 Security of WLANs

The book named ‘Hack proofing your Wireless Network’ was published by Susan [6]. The book was written on countermeasures and the security issues relating to 802.11b WLANs.

The security issues covered in this book ‘Hack proofing wireless network’ include the published WEP flaws and configuring the networks poorly. Countermeasures offered include several which might be implemented immediately with no monetary outlay but extend to measures should be put in place to protect critical data transmissions. Barnes claims that I is possible to to implement and maintain a highly secure WLAN but many will rush to implement these solutions without spending time to understand all of the possible threats and security precautions that should be taken to mitigate them. For this result, misconfigurations will likely result in the downfall of security.[6]

In the past before the publication of Barnes book, there were several papers that claimed that 802.11b compliant WLANs, it is needed to secure third-party solutions to implement it.

At the department of Computer Sciences, University of Maryland, published a paper on March 30,2001 with the title ‘Your 802.11 Wireless Network has No Clothes’. The research paper the described the weaknesses of 802.11 specified shared key authentication mechanisms. The research paper mentioned that ‘All of the deployed 802.11 wireless network are at risk of compromise’ and they recommended that there be a Major overhaul of the current standard. [7]

The National Institute of Standards and Technology (NIST) which is a part of U.S Department of Commerce, in September 2002, published a report with the titled “Wireless Network Security” [8]. It was showed the overview of wireless technologies, followed by the detailed information concerning the problems with 802.11b security, including mitigation and the countermeasures to deal with these problems.

Later after that month, a draft report entitled the National Strategy to Secure Cyberspace (2002) was released by the U.S presidential Administration, which was intended for federal departments and the agencies. It was stated in that report that the Bush Govt. asked federal agencies to exercise

extra caution when using a WLAN and recommended that they install more encryption than would be necessary on a wired network.

3.3 IEEE Standard

The 802.11 b standard defines the WEP algorithm as "a fonn of electronic codebook in which a block of plaintext is bit~wise XORed with a pseudorandom key sequence of equal length. The key sequence is generated by the WEP algorithm" [6]. XOR or "exclusive or" is a mathematical operator that returns true if one and only one of its operands is true.

The growth of WLAN technology accelerated by the Federal Communications Cummision(F.C.C) of U.S.A by definiing three separete seperate radio operation bands, the industries, the sciewentifice and the medical for the same purpose.

Those three frequency brands also knows as ISM. Boost up the WLAN evaluation as after that, there was noneed for vebdir to have a special license in order its devicess to operate. Earlier in this study it was noted that the IEEE introduced the first WLAN standarsds june 26th of 1997, but since then more standard also introcured to the community. IEEE 802.11b standard was the stard of the WLAN evolution.

New key management and integrity mechanisms were introduced through to WAP2 (IEEE 802.11i) which mantains the management and integrity mechanisms of WPA but ontroduces AES encryption as well as moving much of the security functionality to the hardware that was evolved from WEP to WPA, which is the evaluation of security standardisation of IEEE.

3.4 IEEE 802.11b

This is the stage where three main methods were designed to implement security in wireless network.

- MAC address filtering
- SSID – Service Set Identifiers
- WEP – Wired Equivalent Privacy.

3.4.1 MAC address filtering

In IEEE 802.11 standard, there is no part of MAC address filtering, but it was widely deployed. Each network interfce has a unique MAC address at layer two. This is the method of access control that involes confiquring the access points to only allow authorized MAC addresses to enter the network.

3.4.2 SSID

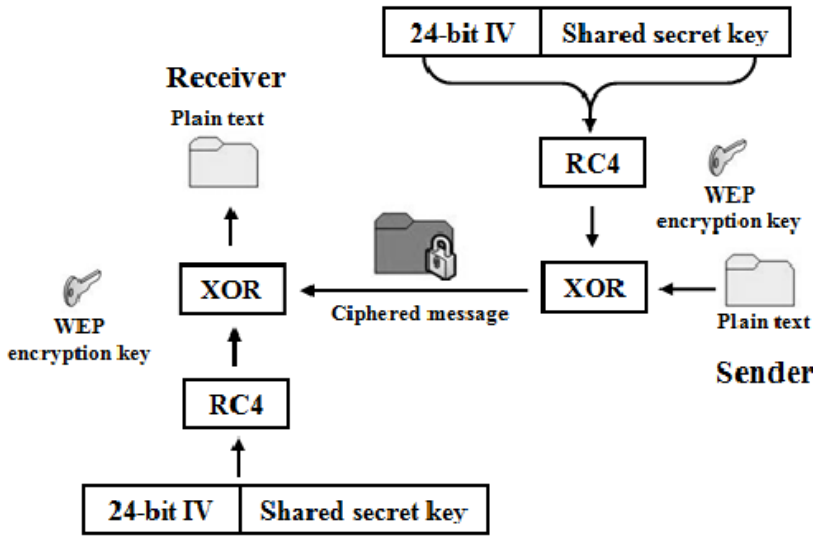
The Service Set Identifiers (SSID) that acts as an indentifier for a particular WLAN. It is a 32 byte or less network name of a service set. There are two modes of operation: open mode and cloed mode. The SSID of thr Access Point is brodcast to the world in the open mode. In the other hard, for closed mode it does not do the same as open mode. It does not react to the messages unless they contain the correct SSID in the message headers. There has to be same SSID for Confiquring if any divice wants to connect to a particular WLAN. The SSID is delivired to the AP in the header of every message in clear text and confirmed by the AP before communication can progress.

3.5 WEP

When the IEEE 802.11 was approved ,Wired Equivalent Privacy (WEP) was also introduced as a security standard. The main aim of this was is to secure the wireless network in the same way that the wired network used to protest security and privacy.

WEP encryption algorithm called RC[V] is based on a strem chiher. It is used to control access to the WLAN and to encryp confidential data for its protection. In the algorithm, the secret key is introduced in WEP algorithm and a 24 bit initialization vector (IV) are concatenated as the encryption/decryption key. After getting the resulting key, its acts as the child to generate the key sequence. After that, text message with its ICV, which is also combined with the key sequence. Finally, we get the cipher text, a bitwise XOR is process and the final encrypted form is made by attaching the IV in front of the cipher text.

The severse process is used for decrypting the encryption process. In the beginning, using the shared key and IV, key sequence is generated by the receiver. Secondly, the original plain text can be resumed by XOR operation between the key sequence and the cipher text. After that the data integrity is seen (checked). The plain text is then sent to integrity algoritm to have a new ICV. At the end we should see the diffrence betweeen the ICV old and ICV new to find out the data integrity according to Alhalsani et. al (2014).



Picture 1. WEP schematics

3.5.1 Attack on WEP network

WEP is now vulnerable to many attacks. Plain text is sent as encrypted packet along with IV.Therefor, the information which is sent out already can be cracked easily by anyone and also can hack the secret key. There is a need of patience to crack the WEP key of the network traffic if only by listening and saving them. There is a process called injaction which is used to speed up the process.It is the process of resending operations repeatedly very faster. And this way, in no time we can identify many IVs . After capturing the IVs , we use this to find out the WEP key according to Tews [9].

There is another disadvantage of this that the IV is sent out with clear text which helps the attacker to recover the actual key based on the rotating 24 bit IV. The IVs are revised when the certain number of frames are done, and it helps it very easier for the cracking WEP key network. And thus, WEP is now considered a weak algorithm.

3.6 WPA

Becasue of the drawbacks and limitations of WEP, the Wi-Fi Protected Access (WPA) is introduced. WPA overcomes the weaknesses of WEP and it is also the part of IEEE's 802.11i wireless security specification. There were several chnages in the security technique for example, the use of TKIP (Temporal Key Integrity Protocol). Also there were changes in IVs, by increasing the size of IV and the use of mix function as Tews [9] mentioned. EAP and 802.1x are being used for the authentication. 64 bit or 128 bit encryption key is used in WEP, by entering manually on WAP (Wireless Access Point) and divices and throughout the process it remains the same. TKIP assigns a per packet key, which means that it automatically creates a new 128 but key for every packet, and this way, it protects the attacks that compromised WEP. But, TKIP is not a strong security protocol and no longer in is use with the standard of 802.11.[10]

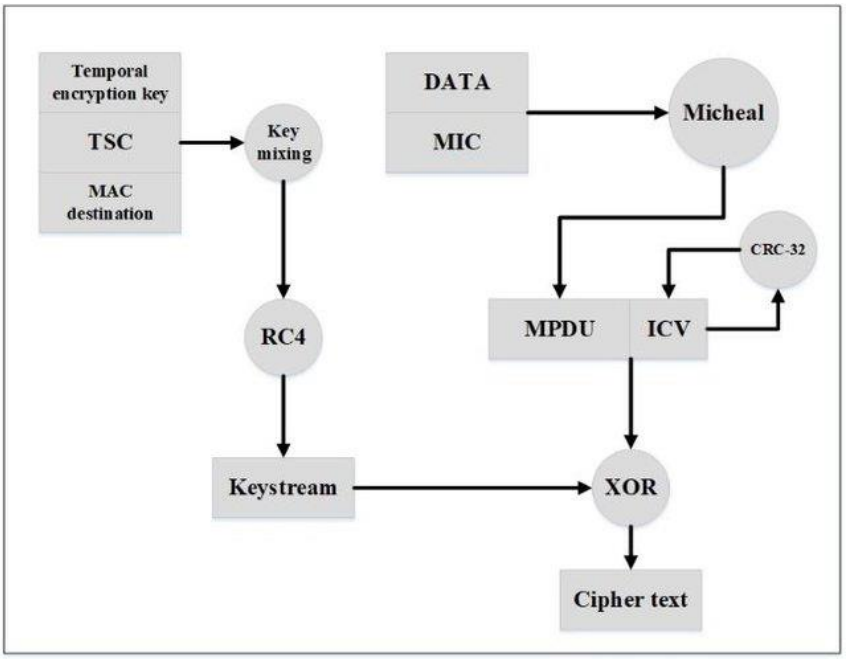
3.5.2 WPA Encryption

For encrypting a wireless data frames we have to go through the follows tasks:

- Initiakization vector(IV)
- Data encryption key
- Source and destination address
- Priority field value
- Data integrity key.

Existing wired equivakent privacy (WEP) is being used and runs as a WEP sub componenet. RC4 and TKIP is used as encryption algorithm along with its 48 bit size. The length of the encrypted key is 128 bit, which is then followed by the integrity check mechanism of Michael algorithm plus CRC-32. In the procedures, A key is used only once and not repeated again and basen on TKIP, the key keeps on changing when every after some data is transfared. To create a key stream, by mixing the input key (TKIP, transmit address , IV, extended initialization vector), it is then combined with clients MAC address. When the result is out , it is then used to encrypt data with the help of the RC4. Michael algorithm also merged message integrity check with MAC service data unit (MSDU). The Cipher text is form with the RC4, key stream and max service data unit (MPDU), integrity check value and XOR'ed . Mac header , IV, KID, EIV, Cipher Text is in the final packet which is then trasnmitted. Temporal keys are entitled during the four- way handshake phase. It is used in both WPA and WPS2 [11].

A simple drawing of WPA encryption process shown below:



Picture 2. Process of WPA encryption

3.5.3 Decryption process of WPA

The IV field is extended after the IV is extrcted from the IV. To produce the per packet key, The IV, DA and the data encryption key are used as the input for the key mixing fucntion. As the input for RC4 PRNG (pseudo random number generator) function, IV and per packet key are used to generate key stream of the same sixe as the encrypted data, MIC and ICV. With the ncrypted data, the key stream is then XORed , MIC and ICV to produce unencrypted ICV< MIC and the data. ICV is then comparred with and canculated with the value of unencrypted ICV. This is then then data is validated [11].

3.7 WPA2 (Wi-Fi protected Access 2)

The WPA 2 is the IEEE 802.11/D9.0 standard securty macanism used currently world wide which has developed by Wi-Fi Alliance with better encryption technique and with srong security features. But Hardware upgrade us required to cop up with WPA2. As like WPA, WPA2 also got two modes of operation which is WPA2 PSK and WPA2 Enterprise. Because of WPA2's 2 based layer, it protests the network also well. The drawback of it that It cannot ensure security of Enterprise alone. WPA2 and IEEE 802.1X (post based authentication protocol for access control) has to be combined to eleminate most of the security concern in the network. Based on the Advance Encrypted Standard (AES), a new encrypted method which is called Counter mode with CBC mac protocol(CCMP) is used by WPA2 and it is much stronger algorithm than RC4. A plain text passpharase which is called the pre-shared key, is a 256 bit key is generated by the WPA2 personal. Combining the PSK (pre shared key) with service set identifier and SSID length from the based on mathematics, for the pair wise master key (PMK), and It is used to create the four way handshake protocol to generate session key between client and the access point. it is then using an Advanced Encrypted Standard type symmetric encryption which works on blocks of data rather than stream. Also, it operates on 128,192,256 1594bits key lengths.The encryption mechanisms happen in many rounds depending upon key length. CCMP (CCM mode Protocol) is an encryption protocol adopted for Wireless LAN devices that involves the standards of the IEEE 802.11i rules to the first IEEE 802.11 standard. CCMP is better data cryptographic encapsulation mechanism developed for data confidentiality and based upon the CounterMode with CBC-MAC (CCM) of the AES standard. it had been created to address the vulnerabilities showed by WEP, a dated, insecure protocol.

ADD (additional authentication data, temporal key and nonce and also CCMP are used encryption. Also, an aligned 48-bit packet number (PN) is employed to create nonce. Cipher Block Chaining Message Authentication Code (CBCMAC) is utilized for integrity (instead of Michael's algorithm).

CCM = CTR + CBC-MAC for confidentiality and integrity. 48 bit IV size is utilized here and *CBC-MAC* for integrity check mechanisms. The WPA2 mac frame is consists of MAC header,

CCMP header, encrypted data and encrypted MIC. Overall, WPA/WPA2 activate protection against forgery and replay attacks

3.7.1 WPA2 encryption

- With the data integrity key and advance Encrypted Standard, encrypt starts 128 bit block, which is obtained from a passphrase of * to 63 characters of ASCII.
- In the next following step, XOR result 1 with next 128 bit block to rennder Xrasult1.
- Then the excrypted Xresult1 is with Advanced Encrypted Standard (AES) and data intergrity key.
- Finally XOR result2 and then the final 128 bit of block data according to Rawat

3.7.2 WPA2 decryption

Decryption process can be formulated in these 4 steps:

- Find the value of the starting counter from values in 802.11 header and MAC header.
- The starting counter value and the encrypted portion of the 802.11 payload are used as an input for the AES counter mode decryption algorithm with the data encryption key.
- The result is the decrypted data and MIC. To yield the decrypted data block, AES counter mode XORs the encrypted counter value with the encrypted data block.
- The starting block, 802.11 MAC header, CCMP header, data length, and padding fields are used asan input for the AES CBC-MAC algorithm with the data integrity key to calculate a MIC o discover if the data is valid, compare the unencrypted MIC with the calculated value of MIC. If the values do not match, WPA2 discards data [12].

WPA/WPA2 Enterprise implements RADIUS or EAP (Extensible Authentication Protocol) for centralized client authentication via other authentication schemes, like Kerberos, token cards, authentication certificates etc. Users are given login credentials which is later required to

connect the network. It provides extralayer of authentication security as compared to the WPA personal mode.

3.8 WEP as a protector

WEP stands for wired equivalent privacy and it is best method for protection in wireless network security. It is also used as algorithm that is used for to get order and protect information with proper transfers. “Moreover, WEP plays role in the main connection between anti jamming and different transmissions. However, WEP also uses some stream clipper like 40 bit and 24 bit with multiple initialization vector and accurate information. Actually, encrypted method and information are playing role like vector among these devices and sent information to the designated vector” [13]. So, these designated receiver and vector gain information that is based on IV and even on WEP.

There are some keys in wired equivalent privacy for the proper area:

- There is conversation of some bits like pass phrase 40 bits that is convert into 24 bits with the initialization stage.
- Secondly, this key has 26 char hexadecimal that plus with 24 bit and is equal to 128-bit wired equivalent privacy.
- Thirdly, it is the ability to send packets with proper authentication.
- Fourth one is the integrity is used as authentication source.
- Owing to all these factors, wireless routers are built at homes with vast majority.

3.8.1 WEP problems

There are number of problems in the wired equivalent privacy:

- There is manual key distribution in wired equivalent privacy. So, central keys management are absent in it.
- If we shared keys with all than we face difficulty for single set of keys
- In wired equivalent privacy, frequent changes are necessary for proper functioning.

- Here is another problem, there is no mutual authentication.
- In it master keys are directly used. So, it is big problem in WEP.
- Clients face weak integrity and become cause lot of troubles.
- There is no protection because clients reuse the data [13]

3.9 WPA

WPA stands for the Wi-Fi protected access. Basically, it is security standard for encrypted data in the wireless network security and rely on the speed of the Wi-Fi for increasing the safety and protection from vulnerabilities. Wi-fi actually has security key in which we put some digits like we can say it a password for the safety of connection. So, this password is the main key for securing internet speed and your device. Wi-fi speed depends on the number of users and even also reliable on the quality of internet connection. Nevertheless, wi-fi is actually used for the computing devices and it make strong alliance with the encrypted data and created high speed with proper signals. Wi-fi is demanding need in present world because of the globalization and digitalization. Wi-fi can be secured with the security key those we put in our passwords for hidden our connections. So, there are multiple techniques for securing wi-fi speed and connectivity. Wi-fi is the best way to reconnecting with the surroundings.

WPA stands for the WI-FI protected access and it is privilege for users not only in short range but also in wide range. Owners can set up an area and provide the access to all customers. It is actually used as security standard in computing world these devices are equipped with all wireless connections. WPA is also makes strong connection when focus on alliance with an encrypted data. It also provides authentications to wired equivalent privacy.

Broadly speaking, WPA, has primary objective for protocol designed and main usage of to create security connections like Wi-Fi access. However, it is almost same as the wired equivalent privacy and offers more advancements and improvements in security challenges and also provides authorized access. “Nevertheless, it is also important to secure WPA and because of cyber crimes and security risks. So, we must protect our internet connection from attacks and wifi router must be with high security like strong passwords put on” [13].

3.10 WPA 2

Broadly speaking, WPA stands for the Wi-Fi protected access 2. It is advance version of the wifi and even we can say that is more useful in this technological world. Though, it is second version and second set up of WI-FI in wireless connections. Because most of the devices are designed in the years of 2006 but this is new advance version. WPA2 also released in the year of 2004 September and it became mandatory since 2006 for all devices. Moreover, it is an upgrade set up of wireless connection and has proper security tools. It has all security requirements. It also provides stronger data connection and it released on the bases of robust security network. It also supported security mechanism with other wifi protected access and details are given below:

There is provision of stronger connection between infrastructure and even ad hoc networks also include not only in encryption but also with the authentication. So, the security protocol was inadequate and even limited in other networks. Again, there is opportunistic key for the roaming data among all other connections and protected access points.

Nonetheless, “WPA2 is certified in the years of 2006 and ordered by an alliance with Wi-Fi. Thus, this certification is providing ensures to al data and hardware manufactured devices” [14]. It is actually, provide two protocols with strong support system like WPA and WPA2.

3.11 WPA3

WI-Fi protected access also makes alliance for the other access points because of advancements and improvements in technology. WPA3 is stands for the Wi-Fi protected access 3, in this improvement we can say fourteen years development in WPA3. Additionally, it is the most magnificent addition in internet world. It provides greater security and protection not only for individuals but also at wider level. It is also true, when we get WPA3 and efficient router we also get more satisfactory and compatible customers. Here is also good development in this router, it also accepts both connection from WPA2 and then WPA3. WPA3 is also provide the advance

programming in the connections and implemented in practically. It also supports the security measures with WPA3 protocols.

Although, WPA3 has more personal encryptions individually and users get satisfaction with personal network. Users cannot stop traffic when Wi-Fi passwords is secured and connected successfully with personal connections. However, if passwords leak-out than customers faced lot of issues than it is not possible to secure the connection.

In the WPA3, ‘for better protection we can add 192 digits for bit security but it is optional in enterprise system. So, this would be the most welcome feature in Governments entities and even larger level like industries and highly sensitive areas’’ [14]. Moreover, it also depends on the radius implementation because 192 bit needs more protection and updates with the passage of time.

3.12 Security threats related to LAN

With addition to lower cast of IEEE methods it is assure that hackers have number of WLANs to be chosen. Number of incidents have been reported which shows that numerous open applications are being used for collection and exploitation vulnerabilities in the IEEE 802.11 that is standard security mechanism called as wired equivalent privacy (WEP) network engineers are asked by wireless sniffers to capture the data packets to examine the problem.

War driving is a process of using device of cellular scanning to find mobile numbers for purpose of exploitation. It is now expanding to laptops and 802.11 client card for the same purpose of exploitation.

WLAN ready is one of the most sold devices of today. Most of the end uses use the default setting and only implement standard WEP security. So, with this basic WEP it would be easy to collect data and to collect sensitive information like users login, account numbers and as well as personal record also.

AP that is a rogue access point is an AP that is placed on WLANS and it is used for interference for normal operations. For example, it is used if (DOS) that means denied of service attacks from

the hackers. It shows that if rogue AP is correctly programmed with WEP key it can easily capture personal or any kind of data of a client. “The most common versions of this rogue AP is one that is installed by employee authorization. Employees install this access point for usage in home and it is without any necessary security configuration on 6the network of enterprise and it causes the risk for networks” [15]

3.12.1 Deployment of access points

Numbers of APs are deployed under firewall according to data. This threat become more visible when there is no authentication or encryption. “Deployed under the firewall, it is possible that AP transferred authorized packets from inside the firewall to outside the firewall. So, it is possible for a potential intruder to get the chance to destroy the inner trust from outside the firewall. Kevin Mantic a prominent hacker used this classic technique” [16]. In order to avoid this WLAN must be delimited from the LAN by staying in any other subnet. A router is an alternative which allow the packets which belong to the address space of the wired LAN to be in the wired network. A bridge can do the task of security hazard as it allows the packets of the wired LAN to be transferred by the wireless equipment.

3.12.2 Criteria

It is obvious that 802.11b standard requires more efficient security mechanism than that of the default mechanism. Criteria of which areas that are very important to be more powerful must established before evaluation of additional techniques are being performed. Following are the criteria that are necessary to the evaluation.

- It is necessary to manage the network high. Large network is being burdened by the administration of keys and MAC-addresses.
- WLAN should not be affected by the extra security implementations.
- Different security levels are required by the number of users or different applications.

- The use of other desirable techniques or implementation techniques might be hindered by the compatibility issues.
- The important thing to be analyzed is the cost of different implementations.
- Enterprise can grow at high pace by the preference of scalability. When networks is able to scale then network will be able to maintain its security.
-

3.13 The Standard Security Technique

There are three standard security techniques will be described and evaluated by using the above given criteria. IPSec is understood by the IPv6 protocol and it is also possible to be used in 3G. The foremost known for its abilities of making a virtual private network over the TCP/IP connections. It might be very easy to be combined with 802.11b WLAN. It remains on the transport level on the OSI model which makes it transparent to all applications. The aim of Kerberos is the user authentication and access control that also needed to be increased in 802.11b. “The robust security protocol is resulted when Kerberos have been around for a while. It remains on the application level and could also be combine with IPSec. Both means IPsec and Kerberos are suited closed environments best. The last technique has been chosen because its purpose is to be used in a non-closed environment for example an internet café motel” [17]. It also stays at the application level in the OSI model and it could also be combined with IPsec.

3.13.1 Security mechanism

In security mechanism, as we know that there are some threats with the implementing different networks, some methods in wireless networking like passwords and smart cards etc all are included. Some tools are also used like radius and Kerberos services.

In the process of client association, the access point of sending beacons announces one or more SSIDs, data speed, and other information. The client sends a probe and scans all channels and listens to flares and responses to the probe from the access point. The client associates the access point that has the strongest signal. If the signal becomes low, the client repeats scanning to

associate with other access points (this process is called roaming). During the association, MAC address, SSID, and security are sent from clients to access points and checked by access points.

The wireless client association to the actual selected access point is the second step in the process of two steps. First, authentication and association must occur before the 802.11 client can pass through traffic through access points to other hosts on the network. Client authentication in this initial process is not as same as network authentication (entering a username and password to get access to the network). Customer verification is only the first step between wireless clients and ACs, and this verification process leads to communication. Standard 802.11 only determines two different authentication methods: open authentication and shared key authentication. Open authentication is just a four-type "Halo" package exchange without client verification or access point, to allow easy connectivity. Together key authentication using a WEP key that is defined static, which is known between the client and access point, for verification.

3.13.2 WLAN VPN

The VPN (Virtual Private Network) protects WLAN by creating a data blocking channel that blocks unauthorized accesses. VPN has a high reputation for its secrecy and protectivity. VPN uses IPSec protection method. The IPSec uses strong algorithm such as Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) to encrypt data and uses other algorithm to certify data package. IPSec also uses digital key to authenticate public key (Gary, 2016). A VPN basically protect every information that comes through its “tunnel”. In every security protocol, always come with encryption. Nowadays, most VPN services use AES method to encrypt data. There is AES 128-bit and AES 256-bit, the bit number stands for the key length and represents the possible number of combinations, it would take a few billion years for today’s fastest computer to crack an AES 128-bit key [18].

When a VPN is used, first the data go through the VPN server where everything cipher method happens and after that the VPN sends it to the designated server that the user wants to connect. When user pings a server to a website, data are constantly sent back and forth over and over, but with a VPN in the middle, the user’s request is the only thing goes through that website, the data

move along the client and the VPN server, therefore the designated website/server does not hold anything sensitive of the user. VPN helps users “escape” out of cybercriminal s/ corporates / governments ‘s “eyes”, secure the connection for users to browse the internet safely.

3.14 TKIP and AES

- TKIP - Temporal Key Integrity Protocol

TKIP is a solution that was developed for IEEE standard, a WEP upgrades module so as to fix the internal security of the RC4 cipher. TKIP uses “hashing” IV against the counterfeiting data package, it also provides protocols to check the accuracy of each data package [18].

- AES - Advanced Encryption Standard

As mentioned above, AES was put into force by NIST (National Institute of Standards and Technology) - a non-regulatory of the United States Department of Commerce. AES uses CBT-CTR and CBC-MAC altogether and their combination is called AES-CCM. CCM is the combination of CBC-CTR encryption method and CBC-MAC integrity checking algorithm [18].

3.14.1 802.1x and EAP

802.1x 802.1x is a special standard port-based Network Access Control (PNAC) connection which is designed by IEEE. 802.1x working environment is both wired and wireless, it provides a verification structure to the designated device. With IEEE 802.1x, when a user tries to log in into the server, that connection will be set in “blocked” status until the user’s authentication from the server is completed [19].

3.14.2 EAP

Extensible Authentication Protocol is a authentication method which consists of:

- User authentication: passwords, certificates
- Handling protocol: MD5, TLS, OTP (One-time password)

4 Practical Part

4.1 Detection and prevention of broken network

To improve home network security, I took some approaches. The first approach was to prevent intrusions by improving the configuration of the home network. A proof-of-concept application is developed that is able to retrieve and assess the configuration of a home network. Practical part describes how the configuration is retrieved and assessed. The second approach was to explore the possibilities of an intrusion detection system (IDS) within a home network. Even if a home network is configured well, then it is still possible that malicious events happen. For example, a malware infected device is connected to the home network. The infected device is able to discover other hosts on the network and infect these devices. For an intruder that has gained access to the home network, a logical first step would be to explore which hosts are connected to the network, and which services these devices run. Tools that do this are port scanners, such as Nmap. I want to see how an IDS can be deployed within the home network to detect such a port scan. [20]

4.2 Intrusion and problematic issues prevention

To determine if a system is secure an approach is to act as an intruder, and see which actions are possible that bring the intruder closer to its goal. Performing an action might enable other actions. It can be seen as a game that has as goal to intrude a system using a sequence of actions. The ‘easiest’ sequence of actions that exists to reach some intrusive goal determines the level of security within the system. This high-level explanation is the idea behind attack graphs. Attack graphs are used to determine for each system state which actions are possible that move the system into another state. I found that modeling a home network accurately enough to determine which exploits are applicable is too difficult. Additionally, attack graphs rely on an up-to-date vulnerability database where is determined accurately, in which state which vulnerabilities are present. Unfortunately, to our knowledge, there is no such database freely available. Therefore, is decided to look for other approaches to assess a configuration.

An attack on a system often consists of multiple actions. Each action exploits a certain functionality or vulnerability in the system to change the state of the network such that another exploit can be applied. Exploits often require very specific preconditions in order to be applicable. An intruder will try to increase his access to the system in order to enable more exploits. In the end, after a chain of exploits the intruder may reach its goal. With the following attack model which was based on the description of Sheyner [She04] I try to create a model to find all possible attack chains. From there I determine which chains pose the biggest weaknesses in the system and formulate recommendations to mitigate these weaknesses. I define the Attack model W = (S, τ, {s0}, S, S, D) as a Buchi model. A Buchi model is defined as follows: Definition Given a set of atomic propositions AP, a Buchi automaton over the alphabet A = 2AP is a 6-tuple B = (S, τ, S0, Sa, Sf, D) with finite state set S, transmission relation $\tau \subset S \times S$, initial state set $S0 \subset S$, a set $Sa \subset S$ of acceptance states, a set $Sf \subset S$ of final states, and a labeling $D: S \rightarrow 2A$ of states with sets of letters from A. Within the system I define three agents I = {E, D, S}. Where E is the attacker, D the defender and S the system under attack. Each agent $i \in I$ have a set of possible actions Ai which it can execute. The total set of actions is defined as $i \in I$ Ai. The attack model W of a home network consists of the following components:

I. H, a set of hosts connected to the network.
II. C, a connectivity relation expressing the network topology and inter-host reachability.
III. T, a relation expressing trust between hosts.
IV. I, a model of the intruder.
V. A, a set of individual actions (exploits) that the intruder can use to construct attack scenarios.
VI. Ids, a model of the intrusion detection system.

Each host $h \in H$ is defined as a tuple (id, svcs, sw, vuls). The id is a unique identifier for each host, which I choose to be the MAC address of the network interface. A host can provide one or more services to other devices on the network. The vulnerabilities in these services can be exploited in order to get more access to that host. Therefore, for each host I also determine the set of services svcs. The entries in this set consist of a service name and a port number. Next to the services that are running there is also other software operating on the host, the set of other software is defined

as sw. The services and software which is running on a host mostly determine which vulnerabilities are present on a host. Therefore, also a set of host-specific vulnerabilities vuls is determined.

The connectivity between host is also important to determine if a certain exploit can be launched from one to another host. For now, I assume that firewalls can restrict the network traffic on port level. Therefore, I define connectivity as a ternary relation $C \subset H \times H \times P$ where P is an Integer port number. Here C (h1, h2, p) means that host h1 can reach host h2 on port p.

A host h1 can trust another host h2. This means that host h2 has access to host h1. For instance, a device can store the credentials of a Wi-Fi network if it has logged in. From that moment anyone who has access to that device can access the wireless network.

Agent i ∈ I	S_i	A_i
E	*I*	*A*
D	*Ids*	*alarm*
S	*H x C x T*	*∅*

Table 1. The agents with their actions

I want to model the state of the intruder in some way. The actions that an intruder can perform also depend on its gained knowledge. Important knowledge for an intruder to start with is which hosts are available on the network and the logical topology. If the intruder gains knowledge about this, he or she can identify vulnerable hosts and the entry points of the network. The intruder's knowledge also includes login credentials of users within the network. With this information the intruder can impersonate as a legitimate user in order to get the same privilege level as that user. To quantify the privilege level of the intruder I also include in the intruder's model the privilege level to each host. I define this privilege level as the function plvl: $H \rightarrow \{none, user, root\}$. There is a strict total order on the privilege levels: none $\leq$ user $\leq$ root. With the root privilege level, I mean that this user has full access to a device, while with user level privilege there are some restrictions. If the privilege level is equal to none there is the same level of privilege as a user which is not authenticated.

Each action that can be executed by an attacker is defined as the triple (r, hs, ht). The attribute r is a rule that describes how the intruder can affect the system and which information he obtains. This rule consists of four components:

- intruder preconditions: Specifies conditions about the knowledge and privilege levels of the intruder.
- network preconditions: Specifies conditions about the target host state, network connectivity, trust, services, and vulnerabilities that must hold before an action can be launched.
- intruder effects: An action can give the intruder additional knowledge about the system or can give him additional privilege rights.
- network effects: This component describes the effects that the launched action has on the network.

Next to the action attribute r, I have attributes *hs* and *ht* are hosts in H. These attributes describe the host from where the attack is launched and the target of the attack respectively. An action is typically executed by an intruder, but there can also be an Intrusion Detection System (IDS) available within the network which could raise an alarm. Therefore, I introduce a special type of alarm action which can be executed by the Defender agent.

Many configuration options are possible within a home network, some may be less secure than other. It is not always easy to say if some setting in the configuration is secure or not, because it depends on the circumstances where the system is in. For instance, some device in the home network can run a network service that has a known vulnerability which is exploitable. The severity of this vulnerable service depends on whether the service is reachable from someone outside the home network. In this case there should be checked if there exists a port forwarding rule in the configuration which makes the vulnerable service directly reachable from the Internet. If such a port forwarding rule exists, the overall security of the network gets affected by it. Taking the circumstances of a system into account makes the assessment process more dynamic. To do this, I introduce assessment flowcharts which are used to compose a dynamic assessment. Assessment flowcharts are a model to assess arbitrary configurations of systems. The idea is that a security

expert can, based on a security analysis, design an assessment flowchart. This assessment flowchart can then be executed automatically by the system.

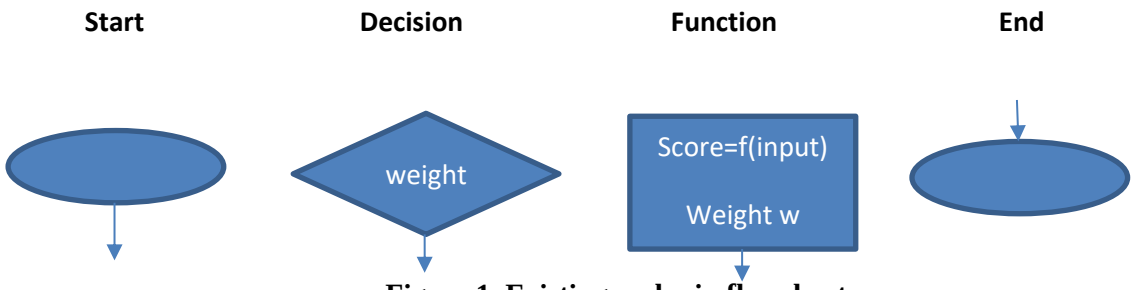


Figure 1. Existing nodes in flowchart

4.3 Components

An assessment flowchart consists of multiple nodes that are connected in the same fashion as a flowchart. The assessment flowchart starts from a single ‘Start’ node and ends into a single ‘End’ node. In between the ‘Start’ and ‘End’ node there are ‘Decision’ and ‘Function’ nodes connected in some way. Figure 1 shows how each node looks like.

- **Start**: Each assessment flowchart has one start node to indicate the start point of the assessment. A start node can only have one outgoing arrow.
- **Decision**: The decision node is used to check a setting of a configuration. Based on the outcome, a decision is taken for the direction the assessment flowchart proceeds. To each direction is a score assigned. The score is a number between 0 and 1 that indicates how secure the setting is. A ‘Decision’ node can have two or more directions in which it can proceed, one for every possible option.
- **Function**: The ‘Function’ node takes some configuration setting as input and determines based on this input a score. As in the ‘Decision’ node the score is a number between 0 and 1 that is used to indicate how secure the setting is. A typical example of a ‘Function’ node is the assessment of a password. The input of a password assessment function node would be the password itself. Based on the properties the given password has, a score is calculated.

- **End**: There is one end node in the assessment flowchart. This node can have multiple incoming arrows but has no outgoing arrow.

To indicate the relative importance between ‘Decision’ and ‘Function’ nodes weights are introduced. For each ‘Decision’ and ‘Function’ node a weight is assigned, which is expressed as a positive number.

4.4 Final Score

The final score of a configuration is calculated by going through the assessment flowchart. For every node on the path a result is calculated by multiplying the weight with its corresponding score. Once the program has traversed the entire assessment flowchart, all results are summed up and then normalized into a value between 0 and 1. Normalizing is done by determining the result of the maximum path within the flowchart i.e. the most secure path.

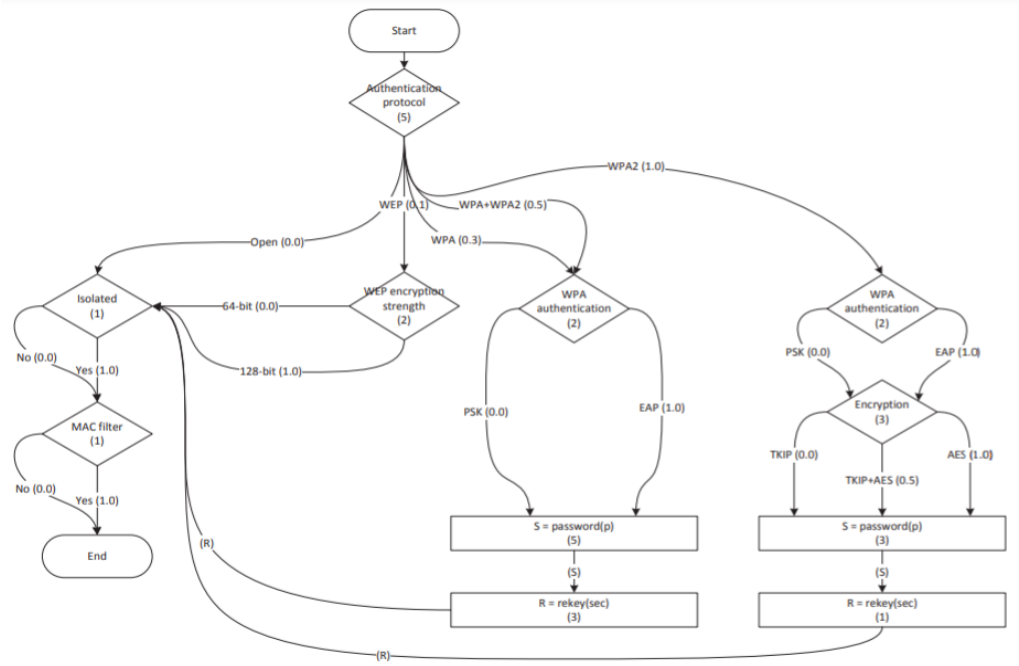


Figure 2. Setting-up Wi-Fi access point

As example Figure 1 shows the assessment flowchart of a Wi-Fi access point which is implemented in the proof of concept application. The first decision node in the assessment

flowchart checks what authentication protocol is used. If the network uses no authentication protocol, it will be assigned a score of 0.0. However, if the access point is configured with the WPA2 authentication protocol it will get a score of 1.0 because it is currently the strongest authentication protocol that can be used for Wi-Fi networks. Depending on the authentication protocol that is used the decision node will proceed in another branch of the assessment flowchart. In this way it is possible to assess a specific sub-configuration of a certain type of configuration. For WPA or WPA2 are for instance different settings to be checked than with an open network.

4.5 Security levels

Once the system has gone through the assessment flowchart a final result is computed. A question that remains is: when is a final result considered secure enough? For this we introduce security levels that provide thresholds for the final results of assessment flowcharts. The thresholds for the security levels can be determined by a security expert. This security expert may for example define three security levels as shown in Graph 1. In this example we get three intervals [0, 0.5], (0.5, 0.8] and (0.8, 1.0] which are mapped to the security levels low, medium, high respectively. An assessment consists of multiple instances of different types of assessment flowcharts. For example, there can be created multiple instances of the assessment flowchart that we saw before in Figure 1, one instance for each wireless access point that is present in the home network. Besides the wireless access point configuration in the network, there can be different aspects of the network be assessed. The result of the program once it has run through all instances of assessment flowcharts is a report with a list of final scores for each assessment flowchart. The overall security level of the report will be the minimal security level of all the assessments in the report.

Security level	Threshold
Low	0.5
Medium	0.8
High	1.0

Table 2. Relevant security levels

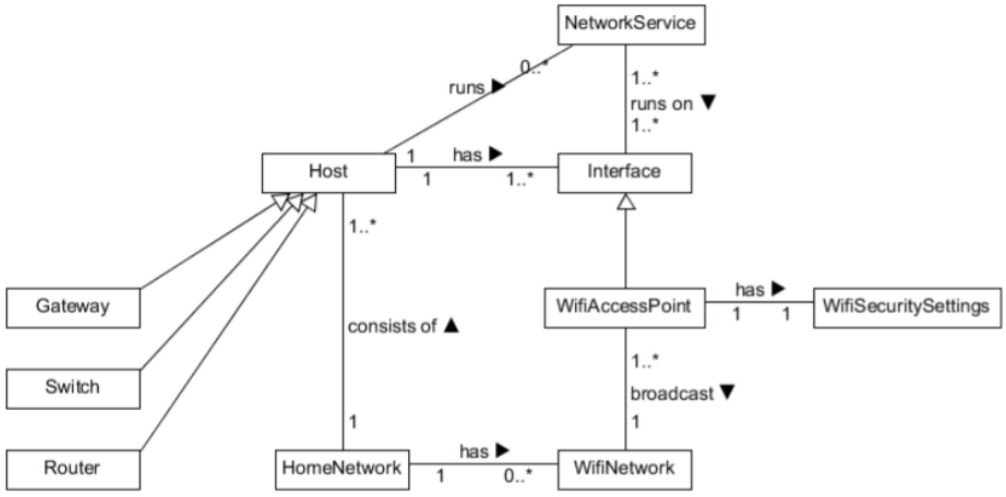


Figure 3. Model of home network

The domain model shown in Figure 2 is designed to store the information that is collected from the devices in the home network. Ultimately this domain model could be transformed into an Entity Relation Model (ERD) such that the data can be stored in a relational database. To explain the domain model, we start at the Home Network entity that contains one or more Host and WIFI Network entities. Each Host entity either can be a Gateway, Switch, Router or a normal host. For every type of device there can be device specific information stored. A Host may run a Network Service such as a HTTP or SSH service. Each Network Service can be provided on one or more Interface entities. For instance, the SSH service for the gateway router might run both on the internal and the external interface, but the HTTP service that provides the router configuration page is only provided via the internal interface. The Interface entity can be a special wireless interface that enables other devices to connect to it. Such interfaces are Wi-Fi Access Point entities.

Wi-Fi Access Points broadcast a Wi-Fi Network using certain Wi-Fi security settings (i.e. entity Wi-Fi Security Settings).

4.6 Password securities

Passwords are still a very common method for authentication. But is this kind of authentication secure enough for the application in home networks? One could argue that passwords are a secure enough method to do authentication in case there is used a strong password. A disadvantage of passwords is that passwords are easily copied, and there is no method to determine how many times this already happened. Passwords might not be a perfect authentication method. However, it is often the only authentication method that is available on a device. Let for now accept that passwords are used as authentication method. To make the authentication as secure as possible we want to assess the strength of passwords. This brings us to the next question: what a strong password is. Steven Furnell describes some commonly used best practices for passwords [Fur07]:

- Use a long password, e.g. 8 or more characters.
- The password should contain both upper case and lower-case letters.
- The password should contain numbers.
- The password should contain special characters.
- It should not be possible that a password can be found in a dictionary.
- Do not choose passwords that someone who knows you is able to guess.
- Do not use choose the same password for all systems you use.
- Change your password on a regular basis.

If a brute force attack is executed an exhaustive search is done over all the possible passwords. When the to be recovered password is 10 characters long and consists of lower-case symbols, upper case symbols and numerical symbols, there are $(26 + 26 + 10)10 \approx 8.39 \cdot 1017$ different possible passwords. Suppose there would exist a 3 GHz processor which is able to check a password every clock cycle. Note that this is already much faster than a consumer-based computer can handle. It would still take about 9 years in order to check all possibilities and 4.5 years on

average. This small calculation would pose that passwords are a strong authentication method. Unfortunately, it is not as nice as it seems to be. People are not very good in remembering difficult passwords and often come up with a password in a common format and, at least, pronounceable. Matteo Dell'Amico et al. show in their paper [DMR10] that, within the password datasets they use, the average password length is around 8 characters. In two of the three datasets around 51% of the passwords use only lower-case letters. The policy of the other dataset enforced the usage of numbers. As mentioned before, people tend to use a common pattern for their passwords. Almost 20% of the passwords in the dataset with the 'enforced-number' policy consisted of lower-case letters followed by a single '1'. Ideally a secure password should apply to all above best practices and is also good memorable. Choosing such a password is not an easy task and could get in the way of the user doing his work. Dell'Amico mentions this as a reason why some users choose to use a weak password [DMR10]. There is a trade-off between usability and security when choosing a good password. To retrieve a password, it is possible to find it by guessing. There are several approaches to do this, every time the challenge is to minimize the number of guesses needed. Checking if a guessed password is correct takes resources like power and time. A rational attacker would only choose to guess a password if the amount of expected guesses g, times the cost c of checking if a password is correct is less than the profit p of a successful password recovery, i.e. $g \cdot c < p$.

To recover a password a strategy could be to perform a dictionary attack. The dictionary attack will try every word in a dictionary file that is provided until the correct password is found. The success probability of the dictionary attack heavily relies on the quality of the dictionary and the type of password that is used. When a random password is used, a dictionary will often be unsuccessful (or the random password consists of a dictionary word by accident).

4.7 Implementation

To find out if the proposed solution would work there is created a proof-of-concept application. The application runs on an Android smartphone and has as main functionality to improve the configuration of a home network. The application requires the smart phone to be connected to the home network. The application is designed to do its job in four stages. The first stage is about information gathering and collects information about the configuration of the network. The

information is gathered by observing the network where the host is connected to, but also by logging into network infrastructure devices such as: routers, switches, and access points. Once the system finished gathering information it will proceed to the assessment stage. In this stage several components get assessed which in the end will result in an assessment report. After the assessment report is generated the application should give suggestions to improve the security of the network in the suggest recommendations stage. Unfortunately, this stage is not yet implemented in the current implementation of the application. After the suggest recommendations stage the application should enter the apply configuration changes stage. In some cases, the application will able to apply some of the recommendations to improve the home network configuration itself. Figure 3.6 shows a summary of the phases that the application runs through. In the following sections we will discuss the stages in more detail in a chronological order.

4.7.1 Information gathering

The information gathering stage collects data about the home network configuration from different sources. Because the device that runs the application is connected to the home network, already some information can be extracted by the device itself. For instance, if the device is connected via Wi-Fi, it can determine what security protocol is used for the wireless network. Another way to retrieve information about the home network configuration is by logging into network infrastructure devices. This is a very accurate method to retrieve the configuration of a certain device. Besides that, to apply the configuration in a later stage it is also required to login into the device. A disadvantage of this approach is that different devices will use different protocols manage the device. Some might only support configuration via a webpage while others also support configuration via command-line over SSH or telnet. There is much disparity between network infrastructure devices and there is no standardized configuration interface available. This causes that custom support has to be built for every different device. There may be many different devices supported, while only a small subset of these supported devices will be present in the home network. To reduce the size of the application a plug-in mechanism could be used in combination with a central repository that contains plug-ins for support for a certain device.

4.7.2 Assessment

After the required data about the home network configuration is gathered the application proceeds into the assessment stage. In this stage several aspects of the configuration are assessed by the system.

4.7.3 Generate recommendation

For some recommendations that are done by the previous stages, it may be possible to apply them automatically by the program. To change the configuration of home network devices it is required for the application to log into the device.

4.7.4 Intrusion detection

To examine if intrusion detection can be done within home networks, we defined two events of malicious behavior to detect:

1. a host performs a port scan in the network.

2. a wireless host injects a forged de-auth package into the wireless network.

The reason to select port scanning as malicious event to detect is because it's a common reconnaissance action to get an impression about the hosts present in the network including the services they run. Port scans can be done in all kind of ways but are certainly not something a normal user might do. The second malicious event is the de-auth package injection attack on a Wi-Fi network. De-auth packets are used by the access point to disconnect all its connected devices. Normally the access point only sends these messages in case of an expected reboot. An attacker is able to forge and inject de-auth packages using freely available software such as Aircrack-ng. The de-auth packages can be used to perform a DoS attack by continuously sending these packages. Another possibility is to enforce devices to re-connect to the access point. The connection between a Wi-Fi device and WPA or WPA2 Wi-Fi access point is established using a WPA handshake. Once the attacker is able to capture one or more of these WPA handshakes he is able to perform a brute force attack to retrieve the password. To detect this attack a wireless intrusion detection system (WIDS) is required, which belong to a different class of devices.

4.7.5 Gateway router

The gateway router is assembled during the project; the parts were selected to mimic the processing power of a high-end gateway router that is on the market within five years. The device has two Ethernet interfaces to connect to the home network part of the setup and to the Internet part of the network. Besides that, the gateway router also has two Wi-Fi interfaces, one to set up as access point, and the other to set up as monitoring interface. The gateway router's operating system is a minimal installation of the Linux distribution Debian, version 8.1. Debian is not a router distribution, so to make the system function first some modifications had to be done.

The basic steps that were taken are:

- Enable forwarding of traffic in the Linux kernel. By default, the Linux kernel drops all traffic that is not destined to the machine itself.
- Setup the IP tables firewall such that all traffic from the Internet part of the setup is blocked, unless the connection is instantiated from an internal host.
- Configure the wireless interface as an WPA2 access point.
- Install and configure a DHCP server such that the hosts connected to the home network part of the setup. Once this was done the system functions as a gateway router.

4.8 Overview deployment

The test setup already mimics a possible real home network. It has a gateway router that connects the internal home network to an external network. And besides that, the network has both a wired and a wireless part that are unified as a single network. Any host, no matter if it is connected via Ethernet or Wi-Fi, can connect to any other host within the home network. Now the network is ready for the IDS and the WIDS to be installed on the gateway router.

4.8.1 Breaking WEP keys

Since the protocols used when communication in 802.11 environments, must state which security protocol is used during the transmit, a user listening to such a communication can easily detect

what encryption scheme might be used. If the used scheme is WEP, breaking the key and decrypting the packet in order to view the contents is no harder than passively listening for packets a couple of minutes and then run a program that breaks it. If the communicating parties use a higher level of encryption, the contents will still be encrypted, which not necessarily means that the packets can be decrypted, even if the WEP key is found.

4.7.6 Attacks against WPA

Using WPA, the encryption scheme is magnitudes better than WEP. WPA uses the TKIP implementation so breaking the key is a lot harder than for WEP and requires brute forcing the packets with a dictionary attack. Fortunately, the number of packets gathered to break WPA is limited to just a couple. WPA has a four-way handshaking procedure between the client and AP where the challenge text and other parameters are passed, and if this handshake is captured, a brute force attack against it might be possible. Of course, in order for the client in question to become disconnected from it. It most likely will reconnect to the AP and once again, the four-way handshake procedure will be passed back and forth and can be captured by a monitoring client. [21]

4.9 Setting up the IDS

The installation of an IDS requires an analysis of the type of traffic that is expected and where to place such an IDS. IDSs can be configured specifically for a certain.

4.9.1 IDS Placement

The Snort IDS is able to run multiple instances distributed over multiple hosts on a network. Each instance monitors traffic passing by on a certain interface (e.g. Wi-Fi or Ethernet interface). In the test setup all Snort instances run on the gateway router. This is a design decision which already creates a restriction on the detection capabilities of the IDS. For instance, the IDS is not able to monitor the traffic between laptop 3 and laptop 4. This is because these two hosts are connected via a switch. If the one host sends traffic to the other host, it will first reach the switch, and then

the switch will forward the traffic directly to the other host. So, in this case the traffic does not reach the IDS, and therefore the IDS is not capable of monitoring the traffic. However, to remain undetected for the IDS an intruder needs to know the topology of the network in order to evade IDS. Usually, the network topology and the location where the IDS is deployed, is unknown to the intruder. Deploying the IDS only at the gateway router may therefore be sufficient to do intrusion detection within home networks. As is shown in Figure 3.9, the gateway router runs multiple instances of the Snort IDS, one on each interface where traffic flows through:

• IDS-1:

- Monitors the traffic that passes through the eth1 interface. This interface is connected to the Internet part of the network.
- IDS-2: Monitors the traffic that is sent over the wireless network, but only on network layer level. Internally this interface is the wlan0 interface. The Wi-Fi interface that broadcasts a WPA2 network.
- IDS-3: Monitors the traffic that passes through the Ethernet interface eth0. This interface is connected to the home network part of the setup.

The lines between the interfaces indicate between which interfaces there is traffic possible. Interface wlan1 is depicted as a dotted line box, this is because it only performs monitoring and is not connected to any network.

4.10 Testing

4.10.1 Software and hardware

To successfully test a brute force attack experiment, there are two components needed: a wireless AP acting as a target of the attack and a client (an attacker) acting as a host with a network adapter capable of monitoring the WLAN traffic, inject packets and performing brute force attack. For our experiments we used laptop Acer Aspire 5738Z with Atheros AR5B91 Wireless Network Adapter as an attacking device. The operation system used on the laptop was Linux distribution Debian

GNU/Linux, since it is an open-source free Linux distribution. Using Linux over Windows provides several advantages: switch the network adapter to monitor mode in order to monitor available WLAN networks is almost impossible under Windows OS. Also, the brute force tool chosen (Reaver) and an Aircrack-ng tools are made to be used under Linux distributions. The Aircrack-ng tool was used to enable monitor mode on the wireless network adapter. Since there is an open source brute-force WPS attacking tool, Reaver, released at, we used this implementation for our tests. To monitor the packet traffic between our laptop and the AP, the Wireshark tool was used.

4.10.2 Reaver

Reaver is an open-source tool for Linux distributions which implements the brute force attack against WPS PIN in order to receive the PSK. The source and free download can be found in." Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.". Reaver in average needs 4 to 10 to recover the target AP's passphrase. In practice, however, it will generally take less than a half of this time. Factors influencing the length of the recovery process are:

• AP type

• Signal strength

• Lockout policy

4.10.3 Brute force attack

To prove our point that performing the attack itself is pretty easy task, as a first part of our experimental part we decided to test brute force attack at home against Zyxel NBG-416N Wireless N-Lite Home Router. This AP was configured to use WPA2-PSK with passphrase 14-60 characters long. Let's assume that the Reaver and Aircrack-ng were both successfully installed and configured on attacking device using apt-get install command. As a first step, we disconnected the laptop from all networks (done in WLAN settings). After that, the wireless card was put into

monitor mode. This was done by using Aircrack-ng utility, airmon-ng. The following command puts the wireless interface into monitor mode:

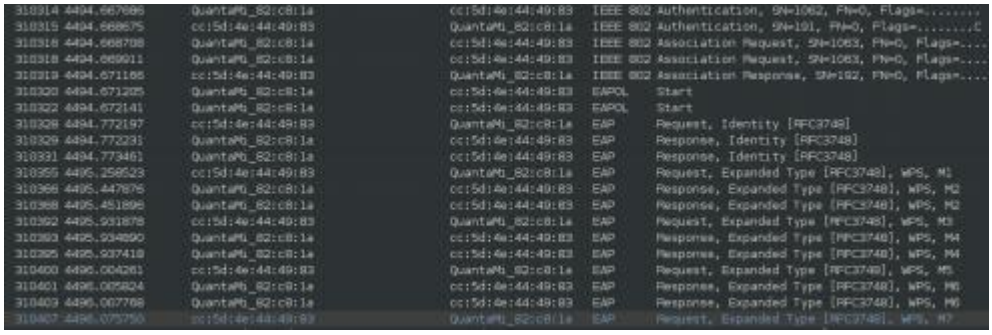
airmon-ng start wlan0

In words, it enables monitor mode on wlan0. On our laptop, the monitoring interface was called mon0. To monitor the network traffic, the airodump-ng tool was used:

airodump-ng mon0

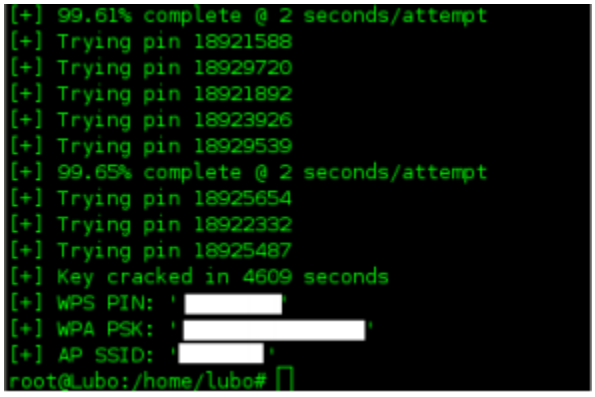
This provided us with the list of wireless networks in range of our laptop. After finding the BSSID of the targeted network, we started Reaver to perform a brute force attack against PIN:

reaver -i mon0 -b XX:XX:XX:XX:XX:XX



Picture 3. An Example of Frames by WireShark

After the attack is successfully completed, we can see the following results in shell: PIN, PSK and BSSID of the target network. We can see the result of the attack on picture 4.



Picture 4. AN example of Reaver output

To prove the fact that the time needed to successfully complete the attack in same conditions is basically random (depends mostly on how fast is the first half of PIN guessed), we've repeated the attack 10 times with various PSK lengths and characters used. The results achieved are summarized in the following table:

No.	PSK Length	Duration
1.	14	96 minutes
2.	14	77 minutes
3.	63	226 minutes
4.	63	119 minutes
5.	47	204 minutes
6.	47	112 minutes
7.	25	84 minutes
8.	25	265 minutes
9.	20	189 minutes
10.	20	106 minutes

Table 3. Attacks on WLAN

It is worth noting that even though the estimated average time of an attack is 4-10 hours [35], during our tests there were attack attempts which were way out of this range- the attack was completed much faster. It was caused mainly by the fact that in these attempts we achieved almost ideal conditions for performing an attack: maximum strength signal, decent router CPUs capabilities, and no error messages (no lost frames, no timeouts occured) resulted in very fast PIN attempts (a little less than 2 seconds per one). At this rate, even the worst possible scenario (generating all 11.000 possible PINs) would take less than 6 hours to complete.

4.10.4 Attacks on WLAN

In order to supply our work with some more data, we tried to test the attack on more than just one WLAN which was configured for that purpose. In order to do that, we were given a permission to perform attacks on wireless networks in two different organizations located in Prague, Czech Republic (although due to legal reasons we are not eligible to provide the names of the organizations).

Organization A

In the first organization, there were 13 wireless networks detected in the building. After quick research we found out that only 8 of them were potential targets of our attack: networks using WPA/WPA2 in PSK mode. It was further confirmed by a system administrator of the company that none of the targeted wireless networks contains more than just one AP.

From the rest, 4 of the networks were encrypted by WEP and one was not using any encryption at all. To act as an attacker, we tried to perform attacks from the public section of the building: the section, which is not restricted area for employees only or is located outside. This approach caused considerably weaker signal strength on some of the target APs (signal strength varied from 34% to 76%). Due to such a low signal strength, a successful attack took longer than the attacks performed in previous section. From the 8 WLANs we tested attacks on 6 were not successful: after an authentication the program could not test PIN requests (EAP messages), which means that the AP did not support WPS or it was turned off - in this case it was confirmed by an administrator that the APs are few years old and therefore they do not support WPS.

On the remaining two, the attacks were completed successfully in 422 (averaging 3 seconds/attempt) and 602 minutes (averaging 5 seconds/attempt) respectively. If we compare achieved results with the results from the previous section, there is a considerable increase in duration of attack caused by lower strength signal.

Organization B

In the second organization we were able to move freely around the building, since there were no restricted areas. From 21 wireless networks found in the organization, 14 were marked as potential targets. The rest of them were again using either WEP (2 networks), no encryption (1 network) or WPA/WPA2 in the Enterprise mode (4 networks). We tried to brute force all WLANs with the following results:

- 11 of the WLANS were not vulnerable to WPS brute force attack.
- 3 of the WLANs were successfully attacked while the PIN and PSK were both recovered.

The results we achieved could be considered only as a minor security threat for the organization because:

- Majority of the WLAN users1 can connect and use the WLAN safely, since the biggest (and most used) networks were being used in the Enterprise mode.
- The small local WLANs, which were vulnerable to our attacks, are being used only by small groups of users. It does not automatically imply that there is low or no chance of capturing important data, but we can nevertheless assume that with more users being potential targets the attacker's chances would be considerably higher

4.11 Results

The combination of the IDS and the WIDS show to be effective in detecting a port scan and a de-auth attack. However, the performance depends on where and how the IDS and WIDS are deployed. The placement of the IDS on the router gateway seems to be adequate to do detection in a home network. Because of the presence of switches in the home network infrastructure, the IDS is unable to monitor all traffic that flows through the network. This reduces the detection capabilities of the IDS. However, it still is an improvement on the security of a home network since, currently, no detection of malicious traffic is done at all. The deployment of a WIDS seems to be more troublesome than for an IDS. This is because it is difficult to cover the entire receiving area of the Wi-Fi devices that are connected to the home network AP. Deploying the WIDS solely on the gateway router will cause that some attacks will remain undetected. However, the same reason as for the IDS applies, deploying an WIDS is still an improvement on the security of a home network because, usually there is no detection done at all. Both the IDS and the WIDS are capable of detecting many more types of attacks than the attacks that are tested during this project. For the Snort IDS there is a tool Pulled pork that updates the Snort rules dataset. In this way the IDS is capable of detecting recent attacks. The Kismet WIDS does not have such an update mechanism. The necessity is less, because fewer attacks on Wi-Fi protocols are developed than on other network protocol.

In practical part, I performed an experimental part. The tests we were able to perform confirmed several thoughts we described in the previous chapter:

- It is possible to abuse the WPS implementation flaw to get full access to the wireless network.
- To do such a thing, all the potential attacker needs is a device with wireless network adapter, which is capable of injecting packets and monitoring traffic, and a little knowledge of working with any Linux distribution (since it is possible to boot Linux operating system from CD/DVD/USB, it is even easier).
- If the attack is not successful or possible, it is most probably caused by one of the following reasons:

– The target AP does not support WPS or it is turned off manually on the device. Since the WPS is enabled by default on majority of devices which support WPS and regular users would not turn it off, the unsuccessful attack is more likely caused by the fact that the device is older and it does not support WPS at all.

– The target AP implements a lockout policy, which makes a brute force attack impractical/impossible. However, during our tests there was no such a device targeted. Either the attack got going and did successfully end or it did not start.

– The target AP is being used in an Enterprise mode, which is not vulnerable to WPS PIN brute force attack.

Furthermore, our results support the assumption that in many companies (excluding those using only one network in Enterprise mode) there is going to be an AP which is vulnerable to this kind of attack. That means that there may be a weak spot in an otherwise good protected network, which enables malicious attacker to access confidential information.

4.12 Solutions to maximize WEP

- Using a 128-bit WEP key:

Normally, WEP devices allow their keys to be configured at: 40-bit, 64-bit and 128-bit. Using a 128-bit key will increase the data package that cybercriminals need to collect for analyzing IV, 128-bit key will cause delays and prolong the time to crack the WEP key.

- Change WEP key regularly:

Changing the WEP key regularly to prevent the WEP key from being exposed while it is in use and make it harder for cybercriminals to focus on a single WEP key.

- Using statistical data analysis tools:

Since WEP key cracking application needs to gather a large amount of data packages and cybercriminals may have to use a tool that boosts up the data package, there should be a booming in data package if someone tries to crack the WEP key. Using such statistical data analysis tool can help the server manager find out and apply countermeasures.

5 Conclusion

To sum up, each device that is connected to a home network can potentially contain private data such as: documents, photos, videos etc. Some of these devices also have additional sensors, such as microphones or cameras. If an intruder would retrieve access to such device, he/she is potentially able to confiscate the privacy of the user in real-time (e.g. when the intruder is able to view the webcam images). It is also important that network infrastructure devices such as routers, switches and Wi-Fi access points are protected. Once an intruder gains access to these devices he is potentially able to setup a man-in-the-middle situation where he/she can affect the confidentiality and integrity of secure connections. We defined two profiles of hackers that could have a motivation for intruding a home network: the curious neighbor and a member of a criminal organization. The entry points that these hackers would use to get access to the home network will be the following:

- Gateway router
- Intermediary device
- Wi-Fi network

To secure for attacks to these entry points it is important that the home network is properly configured. This belongs to the approach of intrusion prevention. Assuming that the home network is properly configured, malicious events are still possible. To do intrusion detection by monitoring network traffic in real-time, there exist Intrusion Detection Systems (IDS).

To improve on intrusion prevention in home networks there is aimed for the use of existing techniques that are already available by the home network infrastructure. This comes down to checking a home network configuration, posing recommendations and finally instrument network infrastructure devices to make improvements on the home network. An Android proof-of-concept application is made that can retrieve the configuration of a DD-WRT router. Based on the retrieved configuration the Android application performs an assessment. To create these assessments we introduce assessment flowcharts, which is a model to assess an arbitrary configuration. The idea behind it is that a security expert creates such an assessment flowchart, and that the system can

execute it. The implementation of generating recommendations and instrumenting infrastructure devices still needs to be done.

For the intrusion detection part of the project, we investigated the possibility of using IDS in home networks. To demonstrate the ability to detect attacks there is built a test setup of a home network. All the equipment used in the test setup consisted of consumer level devices, except the gateway router. Current consumer level gateway routers do not have enough computing power to run additional resource intensive tasks such as running a IDS. Therefore, a gateway router is built that should have the processing power of a high-end gateway router that is on the market within five years. We limited our scope of intrusion detection to two attack scenarios:

- detect a port scan on a host;
- detect a de-auth attack on the Wi-Fi network.

These scenarios were used to investigate and demonstrate the detecting capabilities of these IDS. To detect port scans, we deployed Snort IDS including on the gateway router. For the detection ratio of an IDS its deployment location is an important factor. The IDS must be able to monitor sufficient network traffic in order to perform well. Experiments were done to see from which source host to which destination host, the IDS can detect a port scan. In almost every experiment the IDS was able to detect the port scan. The only experiment where the IDS was unable to detect the port scan was when the source and destination host were connected to the same switch. This was expected because the IDS is not on the route in between the two hosts. Therefore, the traffic of the port scan never reaches the IDS.

My experiments on the test setup show that intrusion detection is possible within home networks. However, the deployment process requires expert knowledge about where to place the IDS instances and how to configure them. Also, the detection alarms of an IDS have to be made more meaningful to the user. Preferably the system should take actions by itself in case of a detection of a malicious event and notify the user about this action.

6 References

[1] KAUTTO ERNBERG, NILS, 2021, Analyzing Google SERP: Swedish Search Queries. *DIVA* [online]. 2021. [Accessed 5 March 2021]. Available from: http://lnu.diva-portal.org/smash/record.jsf?pid=diva2%3A1374908&dswid=3439

[2] KONIDARIS, AGISILAOS and KOUSTOUMPARDI, 2018, The Importance of Search Engine Optimization for Tourism Websites. *Ideas.repec.org* [online]. 2018. [Accessed 6 March 2021]. Available from: https://ideas.repec.org/h/spr/prbchp/978-3-319-67603-6_15.html

[3] TRINH and COLE, 2017, Secondary data analysis: techniques for comparing interventions and their limitations. *Scholar.harvard.edu* [online]. 2017. [Accessed 5 March 2021]. Available from: https://scholar.harvard.edu/apcole/publications/secondary-data-analysis-techniques-comparing-interventions-and-their-limitations

[4] PARADIS, O'BRIEN, BANDIERA and NIMMON, 2016, (PDF) Design: Selection of Data Collection Methods. *ResearchGate* [online]. 2016. [Accessed 7 March 2021]. Available from: https://www.researchgate.net/publication/299461414_Design_Selection_of_Data_Collection_Methods

[5] CISCO, 2008, Authentication Types for Wireless Devices. Cisco [online]. 2008. [Accessed 4 March 2021]. Available from: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html

[6] SUSAN, 2013, Wireless local area network security: an investigation into security tool usage in wireless networks. *Ro.ecu.edu.au* [online]. 2013. [Accessed 3 March 2021]. Available from: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1240&context=theses_hons

[7] ARBAUGH and HOUSLEY, 2021, Security problems in 802.11-based Networks. [online]. 2021. [Accessed 2 March 2021]. Available from: https://www.researchgate.net/publication/220422747_Security_problems_in_80211-based_Networks

[8] DEVICES, OWNES and KARYGIANNIS, 2003, Wireless Network Security Wireless Network Security Wireless Network Security Wireless Network Security. [online]. 2003. [Accessed 4 March 2021]. Available from: https://www.researchgate.net/publication/2590224_Wireless_Network_Security_Wireless_Network_Security_Wireless_Network_Security_Wireless_Network_Security

[9] TEWS, 2007, Attacks on the WEP protocol. [online]. 2007. [Accessed 5 March 2021]. Available from: https://www.researchgate.net/publication/250142546_Attacks_on_the_WEP_protocol

[10] LASHKARI, VARELA and SAMADI, 2009, (PDF) A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *ResearchGate* [online]. 2009. [Accessed 15 March 2021]. Available from: https://www.researchgate.net/publication/213219256_A_survey_on_wireless_security_protocols_WEP_WPA_and_WPA280211i

[11] KHASAWNEH, KAJMAN, ALTHUBYANI and ALKHUDAIDY, 2014, A Survey on Wi-Fi Protocols: WPA and WPA2. [online]. 2014. [Accessed 6 March 2021]. Available from: https://www.researchgate.net/publication/290743584_A_Survey_on_Wi-Fi_Protocols_WPA_and_WPA2

[12] RAWAT and ATAULLAH, 2015, Improving wireless security with enhancement in WPA2 protocol. [online]. 2015. [Accessed 2 March 2021]. Available from: https://www.researchgate.net/publication/285430735_Improving_wireless_security_with_enhancement_in_WPA2_protocol

[13] HASSAN and CHALLAL, 2005, (PDF) Enhanced WEP: An efficient solution to WEP threats. *ResearchGate* [online]. 2005. [Accessed 4 March 2021]. Available from: https://www.researchgate.net/publication/4146842_Enhanced_WEP_An_efficient_solution_to_WEP_threats

[14] WONG, 2018, What's the Difference Between WPA2 and WPA3?. *Electronic Design* [online]. 2018. [Accessed 6 March 2021]. Available from: https://www.electronicdesign.com/technologies/embedded-revolution/article/21806819/whats-the-difference-between-wpa2-and-wpa3

[15] WALIULLAH and GAN, 2014, Wireless LAN Security Threats & Vulnerabilities. [online]. 2014. [Accessed 4 March 2021]. Available from: https://www.researchgate.net/publication/269524313_Wireless_LAN_Security_Threats_Vulnerabilities

[16] RODD, 2009, OPTIMIZATION ALGORITHMS FOR ACCESS POINT DEPLOYMENT IN WIRELESS NETWORKS. [online]. 2009. [Accessed 9 March 2021]. Available from: https://www.researchgate.net/publication/259973195_OPTIMIZATION_ALGORITHMS_FOR_ACCESS_POINT_DEPLOYMENT_IN_WIRELESS_NETWORKS

[17] GEIER, 2005, Wireless Local Area Network Security Protocols: Compliance with the IEEE 802.11i Standard. [online]. 2005. [Accessed 5 March 2021]. Available from: https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/7805/2005-reilly.pdf?sequence=1&isAllowed=y

[18] NGUYEN and BAO, 2016, WIRELESS NETWORK SECURITY. *Theseus.fi* [online]. 2016. [Accessed 4 March 2021]. Available from: https://www.theseus.fi/bitstream/handle/10024/148921/Nguyen_Hoa_Gia_Bao.pdf?sequence=2

[19] CHEN and WANG, 2017, Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience. *Wire.cs.nctu.edu.tw* [online]. 2017. [Accessed 5 March 2021]. Available from: http://wire.cs.nctu.edu.tw/wire1x/COMMAG-05-00270-post.pdf

[20] RIJNETU, 2019, 12 Steps to Maximize your Home Wireless Network Security. Heimdal Security Blog [online]. 2019. [Accessed 4 March 2021]. Available from: https://heimdalsecurity.com/blog/home-wireless-network-security/

[21] VIKLUND, 2005, Identifying threats in wireless environment. Diva-portal.org [online]. 2005. [Accessed 29 February 2021]. Available from: https://www.diva-portal.org/smash/get/diva2:1023347/FULLTEXT01.pdf