International Journal for Electronic Crime Investigation

Vol:2 | Issue:2 | April-June 2018

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

IJECI

Digital Forensics Research and Service Center

Lahore Garrison University, Lahore, Pakistan.

Email ID:ijeci@lgu.edu.pk

LGU International Journal for Electronic Crime Investigation
Volume 2(2) April-June (2018)

SCOPE OF THE JOURNAL

The IJECI is an innovative forum for researchers, scientists and engineers in all domains of computer science and technology to publish high quality, refereed papers. The journal offers articles, survey and review from experts in the field, enhancing insight and understanding of the current trends and state of the art modern technology. Coverage of the journal includes algorithm and computational complexity, distributed and grid computing, computer architecture and high performance, data communication and networks, pattern recognition and image processing, artificial intelligence, cloud computing, VHDL along with emerging domains like Quantum Computing, IoT, Data Sciences, Cognitive Sciences, Vehicular Automation. Subjective regime is not limited to aforementioned areas; Journal policy is to welcome emerging research trends in the general domain of computer science and technology.

SUBMISSION OF ARTICLES

We invite articles with high quality research for publication in all areas of engineering, science and technology. All the manuscripts submitted for publication are first peer reviewed to make sure they are original, relevant and readable. Manuscripts should be submitted via email only.

To submit manuscripts by email with attach file is strongly encouraged, provided that the text, tables, and figures are included in a single Microsoft Word/Pdf file. Submission guidelines along with official format is available on the following link; www.research.lgu.edu.pk

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence,kindly contact at this address:
IJECI, Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
IJECI@lgu.edu.pk

LGU International Journal for Electronic Crime Investigation
Volume 2(2) April-June (2018)

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 2(2) April-June (2018)

Malik *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

Effective Prosecution to Support Digital Forensic Evidence during Investigation and Court Proceedings

Aftab Ahmad Malik [1] Engr. Mujtaba Asad [2] Waqar Azeem[3]
Professor Department of Computer Science, Lahore Garrison University (LGU)
Lahore Pakistan[1]
Department of Electronics and Electrical Engineering, Shanghai Jiao Tong University
Shanghai Minhang Campus, China[2]
Senior Lecturer, Department of Computer Science, LGU; Lahore Pakistan[3]
Email: dr_aftab_malik@yahoo.com[1], mujtaba.asad@live.com[2], waqar.azeem@lgu.edu.pk[3]

Abstract:

Firstly, the purpose of this work is to highlight the significance of digital evidence that exists in the form of digital data and is to be presented in court of law. Secondly, how this evidence (the digital information) can be effectively used during investigation process by the investigating agency. Thirdly, essence of keeping up continued liaison by investigating agency with the prosecutor who is to defend the prosecution side in the court. This paper deals with the offences carried out by offenders using computer, internet, digital media, other electronic devices, hacking and tracking the networks to harm the government agencies or private organizations by violating the network or database or cyber security. These offences are normally the frauds related to financial crimes category and illegal transfer of digital currency. Certain crimes of this area are classified as cyber terrorism. The procedure of collection of evidence and presentation in the court is deviant from other criminal cases. The initial digital evidence may consist of data acquisition, databases, data marts, hard disks, computer file systems and records of illegal transfer of money, This paper advocates to employ powerful prosecution in court of law to make the evidence stronger and consistent with the existing law at the investigation stage as well as in court. The focus of this paper is towards banking frauds and cyber crimes requiring forensic evidence to support the task of prosecution.

Keywords: Cyber Crimes, Cyber terrorism, Forensic Evidence, Prosecution.

1. Introduction

This paper deals with offences of criminal and civil nature. With the advent of new techniques of storage and retrieval of information using computer systems, networks, data bases, data marts, data warehouse technology, data mining and cyber space, we need to preserve and use this technology in the area of criminal information systems. According to [1] and [2] in criminal Information Systems, the most important factors to store are Iris code, DNA, face prints

and fingerprints, which are useful to retrieve the records of criminals and part of forensic evidence. The discipline of forensic science [1] helps to get the criminal information hidden in the digital storage devices such as mobile, computers or other electronic media. The information connected with crime or procured from the place of offence can be initially stored then consolidated, interpreted and used as evidence. The rule is raw data is changed into information and the information is converted into knowledge for important decision making or judgments, after proper analysis. For the purpose of analysis of information, one of the tools is provided by biometrics technology [1] for recognition of handwriting, fingerprints, DNA, face prints, criminal images prepared by artists and matters related to encryption and decryption of information, which is to be used as evidence in criminal investigation and court proceedings. Apart from the essence of the evidence to related banks accounts, ledgers, [2] stresses upon using polygraph, DNA, face prints, fingerprints, modus operandi, extracts from databases of criminal as evidence for investigating officer and attorney.

2. Review:

In order to facilitate the presentation of fresh idea presented in this research paper, the following points are required to be reviewed.

2.1 The Modus operandi

It has been emphasized in [2],[3],[4],[5] and [6] to cater a column in criminal database to indicate the modus operandi, which is of great importance. The modus operandi of different criminals may be different but normally a criminal while repeating similar offence adopts previous modus operandi or slightly deviant one. Same trend occurs in groups of criminal.

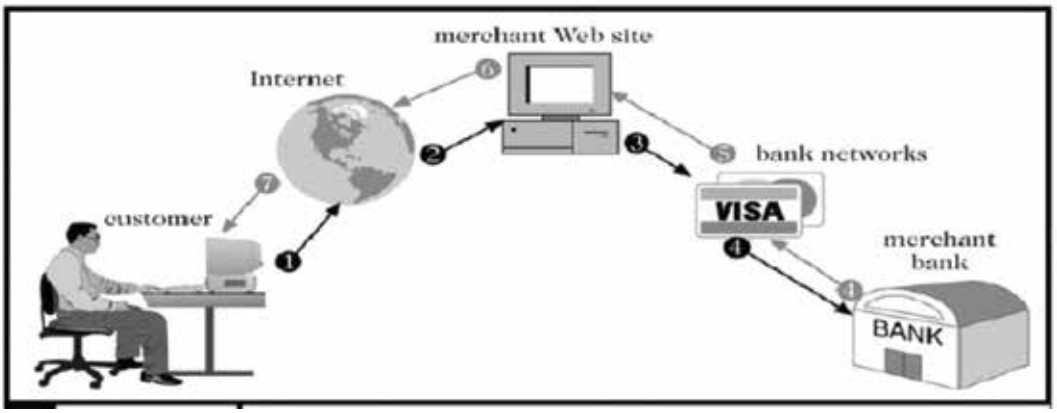
2.2 Financial Frauds and Cyber Crimes

Nowadays most commercial, governmental and private organizations possess computerized management control and information systems for the purpose of storage and information retrieval of their work data. The crimes [2],[3] concerning with using the Computer, internet or electronic Systems connected with Computer networks are categorized as cyber-crimes. The financial frauds are common committed using Cyber facilities by attacking, hacking and tracking into the computer networks systems illegally. There are various ways to commit these frauds such as Email spam, cyberbullying, and committing frauds in on-line business transactions. The security of the computer network systems is of extreme importance and must be maintained at any cost to prevent Data loss, spam emails, hacking and tracking using well known techniques in software and hardware. However [8] proposes to take security measures using firewalls and encryption algorithms.

The purpose of this article is to provide information about cyber security. It gives an analysis that would be useful in taking measure to prevent attacks. The judgment of this analysis is made by expertise and knowledge of databases, hardware, encryption, networks, and firewalls. Moreover it

2.3 Online Payment Systems

Several cyber crimes are committed due to unethical practices during data tractions [9] using online payment systems while customer pays for goods or services. In such systems, we don’t use written checks or cash and transfer the amounts online electronically using methods of mobile and telephone transactions, direct debt from account and electronic money order payment for the billing etc.

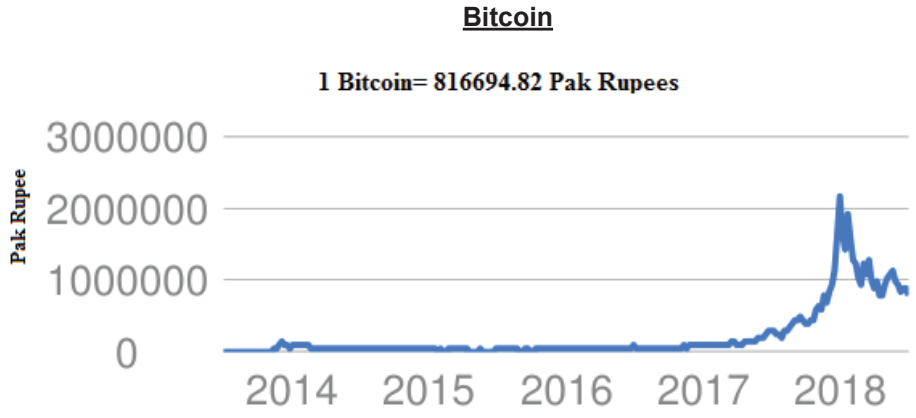


Source: Ritesh Goyal / electronic-payment-system [9]

2.4 Digital Currencies

There exist various digital currencies such as Crypto currency and Bitcoin. The use of the digital currencies has been described by [10] as the online way of transactions by the customer to the merchant for online payment. The digital currencies are called Altcoins. The crypto currency i.e. the Bit coins, Ripple, Litecoin, Tron and Dogecoin etc.

Source: www.moneycontrol.com/cryptocurrency



Source: https://www.coindesk.com/price

2.5 Financial Loss Due to Data Loss

There may be a potential financial loss [11] in using Crypto Currency due to Data loss because it is a virtual currency; therefore, it is inherently risky sometimes. The proposed solution [11] to be on the safe side is to store money in a physical data storage device. There are several offences committed, what is termed as bank fraud. The Central Bank of Pakistan known as State Bank has a supervisory role to play as far as governmental, semi-governmental or private banks are concerned. The State Bank has to implement all rules regulations and monitory, the financial and fiscal policies. The State Bank must take notice where there are irregularities and malpractices occurring in the working of other banks. All government possess inherent trend to help their party members to enjoy undue financial gains through frauds, loans, contracts or illegal allotments. The transactions are to be processed through the commercial banks, therefore, the State Bank under the powers vested, must initiate and take legal action. Most of the times the banks process and deal with false invoices and fictitious/bogus claims of huge amounts. The regime of President Pervaiz Musharraf introduced National Reconciliation Order (NRO) to oversee the malpractices of the past but the Supreme Court of Pakistan declared the NRO to be void and illegal.

3.0 Evidence

According to [2] and [7] the evidence is a fact which can be used in a court to prove another fact. The Law of Evidence, "Qanun-e-Shahadat" was introduced and promulgated in Pakistan in 1984, which defines the categories of evidence such as oral, Circumstantial evidence, Direct, Secondary, Primary or original documentary (public or private). It provides the manner how to present the evidence in the court of law.

3.1 Prevention of Electronic Crimes Act (PECA)

This Act was promulgated in 2016 in Pakistan to prevent offences committed to harm information & cyber systems and to provide legal facilitation and procedure for investigation, prosecution and international cooperation.

4.0 How the Criminals Commit Financial Cyber Frauds?

The financial frauds are committed by causing damage to information system, its access, by changing location, damaging the data virtually using electronic, magnetic, and biometric or any other device. Under the provisions of [12] Prevention of Electronic Crimes Act 2016, the data and passwords are procured by criminals illegally, transaction of data are copied, and interference to data and the information system is caused to commit financial frauds. The damage is also caused by unauthorized interference into one's system or network to alter or spoil the useful information. The offender commits financial forgery or frauds of similar nature of offenses, which have interconnectivity in their approach or modus operandi.

4.1 What Type of Evidence is required by the Prosecutor?

The information gathered during investigation in fraud cases regarding Cyber Crimes must be shared at all stages of investigation and legal opinion of the prosecutor must be obtained. It has been observed that in various court decisions, due to lack of relevant evidence consistent with provisions of law, the courts

have dismissed even the serious cases pertaining to frauds, malpractices, illegal transactions and cyber terrorism. In such cases normally the following type of evidence is essentially required which was used in offence:

- Data on Computer hard disk or CD's or other external cyber media such as internet, intranet or extranet,
- Messages and Emails of criminals,
- Record of Text or voice messages on Mobile,
- Relevant Software to retrieve the information,
- Relevant Record taken from Data Marts, Databases and Data warehouse mined properly,
- Evidence regarding transmission of infrastructure data,
- Data related to on-line-payments
- Credit card No used in fraud,
- Record of Fraud using hacking
- Record of recovered computer files and hard disks ,
- Record of Emails relevant to fraud
- Relevant Image files,
- Procuring complete Transaction Record.

Some of the offences where the above mentioned evidence is essentially required by the prosecutor are computer & internet frauds, frauds using credit card information illegally, counterfeiting, undue financial gains, embezzlements, frauds & thefts in the financial institutions and trading etc.

It is not the responsibility of the prosecutor to investigate guilt and blame of offenders, but the investigating officer is responsible for collection of complete evidence along with the conclusion of the investigation. However, cooperation and cohesion between the investigating agency and the Prosecution is a key to success in court. The defense lawyer can firmly fight out the case, if and only if he is equipped with all necessary information mentioned above. The expert prosecutors having experience in modern technology and law must be engaged who can deliberate on physical exhibits of the case effectively.

4.2 Legally admissible documents be arranged in groups

The subject of legitimacy of evidence is of high significance. There may be hundreds or thousands of documents which are to be exhibited with court file as evidence. This proposes that all the exhibits must be logically arranged into smaller groups keeping in view that how the prosecutor is to defend the case in court. The most irrelevant and legally invalid or inadmissible evidence may either discarded or kept separately for verbal deliberations, if and only if really needed to connect the sequence of fraud or offence. Under the provisions of the the Law of Evidence, "Qanun-e-Shahadat" or Prevention of Electronic Crimes Act (PECA)[13] or any other law, the evidence which is legally admissible can be tendered in the court.

5. Recommendations:

- The prosecutors and investigators must be well conversant with nature and objectives of their profession and gain

adequate proficiency in skills, in the areas of financial accounting investigation and techniques and matters related to conveyancing and pleading in the court of law.

- The investigating agencies and NAB must vigilantly search and investigate where frauds occur or is reported.
- High light criminal schemes of frauds and take cognizance with help of capable and honest investigators,
- Law enforcement must be mandatory for all people specially the influential and high ups,
- The periodic training of the investigators and prosecutors must be made mandatory to improve legal knowledge, investigation skills and norms of court practice,
- The knowledge and skills of investigators and prosecutors must be improved in the area of Computer Science, Information Technology, Software Engineering, Forensic Science, Banking, Law and commerce by introducing short courses in a university.
- The State Bank should not hesitate, because it is duty bound to report all the cases falling within the jurisdiction of National Accountability Bureau (NAB). The cases to be reported on top priority relate to audit reports, bad loans, loans rescheduled and losses caused to the national exchequer by malafide and frauds.
- The State Bank must ensure the implementation of code of business ethics in Banking Sector [14].

6. Conclusion:

The digital and forensics evidence is high significance which must be presented in court of law tactfully, effectively and arranged in logical sequence. The cohesion between investigating agencies and prosecutor must be considered as a strong strategy in cyber frauds and banking sector. Norms of business ethics must be implemented in financial organization in all tiers.

7. Acknowledgement

All the authors are grateful for the appreciation of our work presented in this paper by Mr Kaukab Zuberi Director DFRSC, Lahore Garrison University Lahore.

8. References:

[1] Aftab Ahmad Malik, Mujtaba Asad, WaqarAzeem (2017), “Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed” ; IJECI :International Journal of Electronic Crime Investigation; Volume 1, Issue 1, October-December 2017 Pages 1-10, Lahore Garrison University Lahore.

[2] Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem, DNA Fingerprints Facial Prints And Other Digital Forensics As Evidence In Criminal Investigation and Court Proceedings” ; Volume 2, Issue 1, January-March 2018; Pages 1-10, Pages 1-9; Lahore Garrison University Lahore.

[3] Aftab Ahmad Malik: “Algorithm for

Coding Person's Names in large Databases/ Data Warehouses to enhance Processing speed, Efficiency and to reduce Storage Requirements"; Journal of Computer Science and Information Tech- nology, LGURJCSIT, Volume 1 issue 1, January-March 2017; ISSN 2519-7991

[4] Aftab Ahmad Malik & Asad Mujtaba: "Algorithm for using Codes in place of Facial images during Image Processing in large Databases/ Data Warehouses to reduce storage, Enhance efficiency and Processing speed; Journal of Computer Science and Information Technology, LGURJCSIT, Volume 1 issue 2, April-June 2017;pp 1-9; ISSN 2519-7991

[5] Aftab Ahmad Malik: "Software for Finger Prints Storage and Retrieval of Criminal Identification System for Police", Research Journal, University of Engineering Technology, Lahore, Volume 12; No. 4; PP: 1-18

[6] Aftab Ahmad Malik: Software for Storage and Retrieval of Criminal Information for Police", Research Journal, University of Engineering echnology, Lahore, Volume 13; No.1 PP: 1-28

[7] John William Salmond, " Jurisprudence" , Ebook: ww.ebooksread.com/authors-eng/john-william-salmond/jurisprudence-mla shtml

[8] Syeda Marrium Nizami and Gulfraz Naqvi, " The Reality of Cyber Security ", Vol.1 issue1 Oct-Dec 2017, Lahore Garrison University

[9] Online payment system, https://securionpay.com/blog/e-payment system

[10] Online payment system, https://www.slideshare.net/RiteshGoyal/electronic-payment-system

[11] Mohsin Ali (2017), "Crypto Currency in Cyber world ",; IJECI : International Journal of Electronic Crime Investigation; Volume 1, Issue 1, October-December 2017, Vol.1 issue1 Oct-Dec 2017, Lahore Garrison University, Lahore.

[12] Brian Martucci (2018),"What Is Cryptocurrency–How It Works, History & Bitcoin Alternatives", Posted in: Banking Economic Policy, Money Crash, June 2018; https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

[13] Prevention of Electronic Crimes Act (PECA)

[14] Aftab Ahmad Malik (1995), "Business Ethics in Banking Sector", Book Published by Institute of Banking Sector, Karachi.

Mirza *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

In-Demand Skillsets in Cybersecurity

Jawad Khalid Mirza[1], Zohaib Shahid[2]
Information Security Group
Allied Bank Limited Headquarters
jawad.khalid@abl.com[1],zshahid91@gmail.com[2]

Abstract:

In the recent years, a huge shift to digitization has been observed on a global level. Due to the advantage of having easy access and other benefits, digitization is being adopted fast. With digitization, the ever-growing threat of cyber-attacks increases. Thus, the need for cybersecurity professionals, with an excellent skillset, is on a rise. Alongside this, it is important to know the skillsets of cybersecurity, which are needed the most. This is also important because once an organization knows what skillsets, it requires the most, the spending of its resources will become efficient. As a result, the protection of its digital assets can be done properly. In developing countries, like Pakistan, organizations need to know what skillsets they require the most because many of them have limited resources. Considering this problem, this research makes an effort to list and describe the most in-demand skillsets of cybersecurity in the world. As the skillsets of cybersecurity increase in number and versatility, a good knowledge of what skillsets are required can prevent saturation in the job market. This research will also help people, who are amateurs in this field, understand the concept of cybersecurity and the knowledge required to excel in this field.

Keyword: Cybersecurity, Skillsets, Cyberattacks, Network Security, Cloud Security, Security Analyst, Penetration Testing

1. Introduction

In this fast-progressing digital age, when all kinds of assets and data is being shifted online, the need for qualified cybersecurity professionals is more than ever. It is a critical issue because in this current era of technology, where many advancements have taken place, a negative aspect named cyberwar has also evolved at an astonishing pace. The attackers of today need not plan airstrikes or send an army across a border when they can just reach the sensitive assets via the internet or related technology. With this grave danger in existence, there is still less awareness of cybersecurity and a deficit of qualified security professionals in the industry. Thus, an expert blackhat can break in and eavesdrop on sensitive communication and

steal sensitive data without being detected for months or even years. Even when a security breach is detected, it is not easy to trace expert hackers because they leave no footprints. So, as observed, digital assets are always at a huge risk because they can be affected negatively without any disturbance or noise.

With every passing year, the threats, to cybersecurity, and their sophistication escalates which makes the need for cybersecurity positions a priority within organizations, according to Alice Hill, Managing Director at Dice.com [1]. As the threats evolve, the skills gap becomes wider. According to 'Hacking the Skills Shortage' report by Intel, there will be 1-2 million unfilled cybersecurity jobs worldwide by 2020 [1]. According to [2], 32% of the enterprises report that the time to fill cybersecurity and information security positions is 6 months or more. The percentage of enterprises in USA, Europe and Asia, who are unable to fill open cybersecurity positions are given below [2]. The small percentage in Asia can also be attributed to the fact that in developing countries, like Pakistan, cybersecurity is still a budding field. Organizations are still working to incorporate proper measures of cybersecurity. As more organizations will enter the realm of cybersecurity, the need of cybersecurity professionals will increase and reach the level observed in USA and Europe.

Europe (30%)

USA (27%)

Asia (22%)

Also, 37% of the companies indicate that fewer than 1 in 4 candidates are qualified for such jobs. So it is clear that there is an acute shortage of cybersecurity professionals and skillsets in the industry. Considering that, it is important for one to know about the most in-demand cybersecurity skillsets to train in. The section, ahead, give the details of such skillsets.

2. Literature Review

After an extensive study, it was found out that there is a versatility in the skillsets found in cybersecurity. Every skillset has its own importance and contributes to the whole concept of cybersecurity in its own way. Concerning their requirement, a lot of other factors also come in play like the type of data to be protected, the location of the storage of sensitive data, the approach to cybersecurity (taken by the organization) etc. Some cybersecurity skillsets, which are in the most demand, are detailed below. The order, in which they have been set, does not mean that one skillset takes precedence over the other.

2.1 Network Security

As organizations move to virtualization and cloud technology, the demand for network security professionals has increased a lot [1]. Although network monitoring applications have taken care of a lot of the work like detecting suspicious behavior but an expert person has no substitute. When it comes to threat escalation and developing countermeasures against different types of malware, organizations need experienced employees with excellent knowledge of networks [1, 3]. With the presence of critical infrastructure in business networks and the success of current ransomware, security professionals need to find and repair the vulnerable points in their networks. This skill applies to a wide array of companies like technology firms, consulting companies, government, healthcare and retail [1]. So an up-to-date knowledge of network security is essential to save an organization from multiple

threats.

2.2 Cloud Security

As mentioned before, all organizations have to handle very large amounts of data and need more infrastructure so the use of cloud solutions is on a boom. Although there are a lot of security benefits of this technology but improper use leads to increased data breaches, weak identity management and denial of service [1]. The main issue is that there is a deficiency of personnel with adequate knowledge of cloud security. In a recent Intel security report, almost half of the surveyed organizations indicated that the lack of cloud security skills discourages adoption or usage of cloud services [1]. In a research report by ESG/ISSA, 22% of the respondents said that their organization suffered from an acute shortage of cloud security skills [4]. Thus, the demand for cloud security professionals is only going to increase in the coming time. Coming to the other side of the picture, that is, the cloud service vendors, secure and proper cloud data management is also a top priority. Overall productivity is increased as a result of good cloud data management [3]. As hackers target cloud servers too, cyber security professionals, well-rehearsed in the knowledge of cloud security, are needed by vendors too.

2.3 Data Security

Data security is concerned with the protection of digital data, kept in databases or related locations, from unauthorized users like cybercriminals. The techniques of data protection include data encryption, regular backups, data masking and data erasure [5]. Concerning the ever-increasing amount of data handled by all kinds of organizations, skilled professionals are needed to analyze the need of data security and protect the data accordingly. According to [1], over half of C-level executives said that data security is among the top three business priorities in 2017. Also, the average cost of a data breach is a major concern as it is $5.28 million or 20 percent of the revenue [1]. This is without the consideration of lasting brand damage. Many operations are linked with the data, handled by an organization, so an expert data security professional can help a lot.

Organizations are getting very concerned about data security because of the increasing events of data breaches like the attack on Yahoo in 2016, which compromised 1 billion accounts [1]. In 2017, two largest data breaches, of their kind, took place and did a lot in moving data security to the top of the list of concerns of major organizations. On July 29th, 2017, Equifax, which offers credit monitoring and ID theft solutions, revealed that the data of 143 million US citizens (almost half of the country) had been exposed [6]. The stolen data included the names of the consumers, social security numbers, birth dates and addresses. Driving license and credit card numbers of about 209000 citizens were also stolen. It was later revealed that the sensitive data of 2.5 million additional US consumers had also been stolen [7]. Thus, the number of total US consumers affected, by this massive data breach, went up to a shocking 145.5 million. One of the world's "big four" accountancy firms, named Deloitte, discovered in March 2017 that it had been the target of a major data breach [8]. Lots of conditional information, including the private emails and documents of the clients, was stolen. In both cases, it was found out that the data breach had been occurring for quite some time (months) before it was discovered. As discussed before, this is one of the foremost concerns because a lot of irreversible damage has been done before the discovery.

2.4 Security Analyst

Also known as, SOC (Security Operations Center) Analyst, a security analyst with good investigation skills and experience can save an organization from many threats before they cause lasting damage. According to [4], 33% of the respondents, surveyed by ESG/ISSA, revealed that their organization has an acute shortage of investigation skills and security analysis. Another main issue is that this skillset takes years to develop so organizations usually benefit by luring security analysts from other organizations [4]. Nonetheless, harvesting good security analysts is a need of time and can benefit an organization a lot in the long term. By analyzing the network traffic, an expert security analyst can identify threats properly and can help mitigate them timely.

2.5 Penetration Testing

Through proper work done by penetration testers and ethical hackers, a company can know about the security flaws in its services and applications well before time. A well-trained pentester can identify zero-day vulnerabilities which are the ultimate targets of cybercriminals. Such vulnerabilities allow them to exfiltrate data for months or even years without the organization knowing anything [1]. In the ESG/ISSA report, 20% of cybersecurity professionals said that their organization has an acute shortage of pentesters [4]. Keeping this figure in mind, it cannot be ignored that a comprehensive security policy is only made when extensive penetration testing has been done [1].

2.6 Application Security

Cybercriminals are able to carry out successful attacks due to less awareness and implementation of secure coding. 32% of the cybersecurity professionals, in the ESG/ISSA research report, revealed that their organization suffered from a deficit of good application security skills [4]. For our own ease and usability, secure coding practices are neglected. When software is not patched properly and there are flaws in the code, data breaches become successful [1]. Thus, a professional, trained well in application security, will produce secure software, which will, in turn, protect employees from typical security threats and increase productivity [3]. Also, any secure software should be able to blend with other security measures in the organization [3]. They are not usually convenient but they can keep employees and information safe. Intensive secure code development and quality analysis will cost a lot in short term but as the probability of breaches will decrease, a long term benefit is surely present.

2.7 Risk Management/Evaluation

Excellent risk management is crucial for any organization to protect itself from cyberattacks. By gauging the importance of different assets and services of an organization, the measures for protection can be managed properly. Finding out about the risk, faced by cyberattacks, is a first step towards stopping most threats [3]. Thus, a professional with good risk management skills can save a company a lot of cost in protection of its digital assets through adequate analysis of the risks involved. Also, risk management plays a huge role in internet governance. This is because through the discovery of emerging risks, the norms, shared principles and related elements of the internet are altered which affects its evolution and way of use.

3. Analysis

Concerning the lack of cybersecurity professionals with the required skillsets, there

is a dire need to work on this vector. This is because cyberattacks are increasing exponentially and without trained professionals, they will get out of control easily. In many countries like US, UK, Singapore, India and Australia, the development of cybersecurity professionals has caught a fast pace but Pakistan still lingers behind. Although Pakistan may not have entered the digital age completely but its organizations are affected a lot by cyberattacks.

The cyberwellness of Pakistan can be judged by the fact that it ranks 67th on Global Cybersecurity Index [9]. This means that there is still a long way to go. Cyber legislation, in Pakistan, is still in its infancy but the neighbor, India, got this legislation in 2000 and has been developing quite fast in the field of cybersecurity [10]. Cybersecurity or information security is still a new subject in Pakistan. Only a few academic institutes like National University of Science and Technology (NUST) and Center for Advanced Studies in Engineering (CASE) have introduced Masters degrees and are doing good research work. NUST has also built its own Cyber Emergency Response Team (CERT). Such developments can only be quickened if academia, industry and government work jointly to build a cybersecurity strategy so the country can face the increasing threat of cyberwarfare. There is a need to introduce cybersecurity as a subject in Bachelors Degrees of engineering field so students can realize its requirement in the world of today. Also, it has been observed that students of cybersecurity put in a lot of effort in good research but that research seldom targets problems in the industry. The gap between the academia and industry should be bridged. Students should be given projects or research work, based on the problems of cybersecurity, faced by the industry. Such research will not only solve the issues of the industry but will also be very beneficial for the student's career. In this way, they will have a better idea of the issues to tackle once they start their jobs. Also, organizations, in Pakistan, should start spending more on cybersecurity as it has become the staple need, of today, quite rapidly. As a common man, in Pakistan, is still unaware of the dangers he or she faces online, cybersecurity awareness should be a principal target of every major organization like banks and organizations in the government sector. As observed, Pakistan might be far behind in cybersecurity, as compared to other countries, but the efforts being made, no matter how small they are, will help in catching up with others soon.

4. Conclusion

As observed during this research, the knowledge, required to understand cybersecurity, cannot be attached to something specific. The skillsets, described in this paper, not only require one to understand cybersecurity properly but also have thorough knowledge of computer systems, networks and related entities. These skillsets also show that people from other lines of career like business studies can play an important part too. For example, in the case of risk management/evaluation, professionals, from the field of business studies, can help produce appropriate policies and frameworks once they are trained in the basics of cybersecurity. Overall, for the proper progress and awareness of cybersecurity, it is important for technical and non-technical people, in an organization, to work together to implement it. For any novice in cybersecurity, this research work can help the person catch up quickly on cybersecurity and choose a path to build his or her career. Organizations, especially in

Pakistan, should understand that if they hurry in adopting cybersecurity measures and employ and train cybersecurity professionals properly, they will be able to survive and grow in this era properly.

It should be understood that cyber threats are more of a reality now. They can only be avoided by promoting cybersecurity, as a career, in educational institutes and training interested students or professionals, right from the beginning. If the concept of cybersecurity is introduced this early, it will be very easy to fill the shortage of professionals and skills, faced by the industry. Also, Pakistani organizations should consider spending proper resources on cybersecurity for the development of this field and encouragement of people so they may excel in it.

5. References

[1] A. Bennett, "These Are the Most In-Demand Cyber Security Skills for 2017," 28 February 2017. [Online]. Available: https://techspective.net/2017/02/28/demand-cyber-security-skills-2017/.

[2] ISACA, "State of Cyber Security 2017," 2017. [Online]. Available: https://cybersecurity.isaca.org/info/cyber-aware/images/Cybersecurity-Skills-Gap-2017-1500.jpg.

[3] J. Buntinx, "Top 5 Cyber Security Job Skills In High Demand for 2017 and Beyond," 26 February 2017. [Online]. Available: https://themerkle.com/top-5-cyber-security-job-skills-in-high-demand-for-2017-and-beyond/.

[4] J. Oltsik, "High-demand cybersecurity skills in 2017," 20 December 2016. [Online]. Available: https://www.csoonline.com/article/3152023/security/high-demand-cybersecurity-skills-in-2017.html.

[5] Wikipedia, "Data security," February 2012. [Online]. Available: https://en.wikipedia.org/wiki/Data_security.

[6] M. Kumar, "Equifax Hack Exposes Personal Info of 143 Million US Consumers," 7 September 2017. [Online]. Available: https://thehackernews.com/2017/09/equifax-credit-report-hack.html.

[7] S. Khandelwal, "Whoops, Turns Out 2.5 Million More Americans Were Affected By Equifax Breach," 2 October 2017. [Online]. Available: https://thehackernews.com/2017/10/equifax-credit-security-breach.html.

[8] M. Kumar, "Deloitte Hacked - Cyber Attack Exposes Client's Emails," 25 September 2017. [Online]. Available: https://thehackernews.com/2017/09/deloitte-hack.html.

[9] ITU, "Global Cybersecurity Index (GCI) 2017," International Telecommunication Union, 32017.

[10] A. Raza, Securing Cyberspace For Pakistan, Lahore, Punjab: Information Technology University, 2016.

Sumra *et al.LGU (IJECI)*2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

Enterprise Security of Wi-Fi Networks using Simulation

[1]Hafiz Muhammad Usman Gull, [2]Zaka Ur Rehman,
Department of Computer Science, Lahore Garrison University, Lahore
[1]contact@usmangull.com,[2]zakka727@gmail.com

Abstract:

Wireless network setting is developing into the market, and it is the major way of accessing the internet. Design and security of these networks for an organization need to be considered to ensure mobility and access to each individual is accomplished. In this study, simulation effects of 802.1X with flexible authentication via secure tunneling are performed. Opportunistic key caching which is preferred by many vendors was used to transit the session information from the posterior access point to the prior access point to minimize the hand-off latency to allow continuous connectivity to avoid poor network performance. The simulation process was applied throughout the write up of this article without setting up the pricy real lab-test. After the successful modelling of the network, the outcome will be transferred to the real-life environment. The network simulator software was used to illustrate roaming while Cisco Packet Tracer was engaged in the layout design of the wireless nodes. This research applies to network administrators and engineers across the globe to save time and the cost for the network appliances.

Keywords: Index Terms – Simulation, Security, EAP-FAST, 802.1X, EAP Types, WLAN, RADIUS.

1. Introduction

Wireless is the prescribed portability method for getting to the web by clients. Wi-Fi clients spend around 80 percent of their everyday exercises communicating with wireless gadgets in different errands. The accessibility of wireless fidelity (Wi-Fi) empowered gadgets has made it a needing asset. In everyday operation of an endeavor, Wi-Fi is sent to ensure portability and widen the Wi-Fi scope cell. A few associations are as yet utilizing wired-based systems which don't ensure portability to clients while on strolling from point to point Wi-Fi. This will facilitate the congestion of clients in an association from battling for positions inside a stay with RJ45 links to get to the web. Unique IEEE 802.11 Task Working Groups keep on developing new models to address the issue of clients with respect to the handoff speed, control protection, security of information and nature

of administration. Security is a testing factor in Wireless systems because of its telecom nature. In this situation, the predominant challenge is the security of these Wi-Fi systems. Security challenge turns into an unmanageable issue since information spread is done by means of electromagnetic waves which ricochet over the programmers' region. This notable component makes these systems unreliable not at all like in wired plans where a fraud is requested to have a link network to tap information bundles. Clearly, IEEE 802.11ac and IEEE 802.11ad WIGig are the cutting edge measures of Wi-Fi-based systems that are growing into the market space to furnish the 60GHz with in reverse similarity with IEEE 802.11n which was transcendently intended to help Wi-Fi security highlights. The WLAN IEEE 802.11 conventions were developing as uncovered in Figure 1.

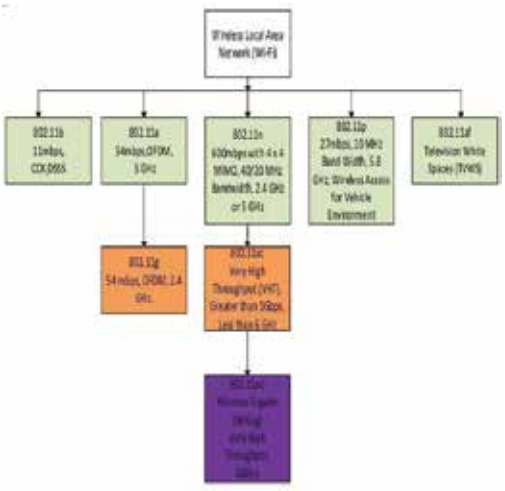


Figure 1 Chronological of IEEE 802.11 Standards for Wi-Fi [3]

Security conventions began to spring into reality in 1999 in the remote milieu. WEP imperfect and its keys recouped. WPA was approved as an interval convention to address the issue of WEP. In 2004, Robust Security Network or WPA2 was formally propelled to supersede WPA. It is the contemporary convention utilized today and all Wi-Fi CERTIFIED contraption confirmed as from 2006 are good to WPA2 and gives Wi-Fi customers' to get to the most progressive and superlative security-based frameworks. Table 1 beneath demonstrates the Wi-Fi Alliance proposed security models conventions highlighting the comparison of WEP, WPA, and WPA2 silent features.

Standard / Features	WEP	WPA	WPA2
Period of Approval	1999	2003	2004
Encryption/Cipher	Assigns the key manually, scramble shared secret keys by employing Rivest Cipher 4 (RC4) nonentity stream	None linear TKIP- based on RC4 nonentity stream	Counter-Mode with Cipher-Block Chaining Message Authentication-Code Protocol (CCMP) of 128-bit AES block cipher
Integrity of Data	CRC-32	Michael (MIC)	CCM
Size of the keys in bit	40	128	128,192 or 256
Scrambling for Packet's Key	Linear hashing	Mixing Function	Scrambling of the packet is optional
Integrity of the header	None	Michael	CCM
Management of the Encryption Key	No	EAP	EAP
Scheme of Authentication	WEP probe a client by a challenge message	802.1X/EAP authentication	802.1X/EAP authentication

Table 1 A Comparison of Wi-Fi Alliance Security Standards Protocols Salient Features[20]

1.1. EAP Authentication Protocols

Since Wi-Fi Local Area Network (WLAN) security is significant and EAP types offer a potential enhanced method for defending the WLAN association, merchants are quickly creating APs with EAP. Table 2 underneath outlines countless EAP norms for Wi-Fi Alliance Accreditation program.

EAP Policies	EAP-TLS	EAP-TTLS	PEAP	EAP-FAST
Authentication	Yes	Yes	Yes	Yes
Delivery of dynamic Key	Yes	Yes	Yes	Yes
Security for Wi-Fi	Very high	High	Strong use of passwords	Medium to High
Rogue AP Detection	No	No	No	Yes
Vendor	Microsoft	Funk	Microsoft	Cisco
Deployment	Difficult	Adequate	Adequate	Adequate

Table 2 A Summary of EAP Types [20]

1.2. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP –FAST)

Cisco EAP-FAST exclusive is implied for the customer server security basic outline to supplant LEAP because of its defects and to offers security as PEAP and EAP-TLS. It is made out of three stages;

Stage 0 - additionally called Automatic Protected Authentication Credential (PAC) provisioning stage. It isn't required since manual provisioning can be utilized. It furnishes the end client with PAC to join the system.

Stage 1 - In this stage, ACS and end-client built up a protected TLS burrow in view of the client's PAC qualifications

Stage 2 - client certifications a safely conveyed utilizing a grouping of sort/length/esteem (TLV)- encoded data from the supplicant to the AS and the other way around. MS-CHAP, GTC, and TLS are the main internal EAP-FAST composes upheld.

The Authentication server, as a rule, a sweep server (Cisco ACS, Funk RADIUS and Microsoft IAS) is utilized to produce PAC by utilizing the ace key and the username of the customer gadget. The segments of PAC include:

PAC – Key: Is a 256-piece pre-ace mystery key utilized by the customer gadget to accomplish the TLS burrow. This key is tough entropy of 32-octet keys subjectively produced by the AS.

PAC – Opaque: Comprises of PAC's critical and companion personality which the server utilizes to recover basic data for approving the validation and of the associate by the server.

PAC – Info: An impulsive length-field used to give minimal expert of character or issuance of the PAC by the predetermined PAC server. This data is utilized to decide the recharging of PAC-Key by the AS.

In this examination, the intrigue is in planning a protected endeavor WLAN that utilizations 802.1X through a RADIUS server utilizing EAP-FAST to upgrade common verification in the connection layer and physical layer to create a safe and propelled encryption standard key. The EAP-FAST's PAC is overseen progressively and reestablished by the verification server. The conveyance of PAC to the client is either done physically by a capacity gadget or consequently through the air. Cisco Wireless LAN Controllers was liked to enroll our entrance focuses and Cisco

Secure ACS server to stores the Lightweight Directory Access Protocol (LDAP) and RADIUS databases. Range/LDAP will be designed to empower a page login instrument. EAP-FAST transmit confirmation information between the supplicant and the AS. EAP-FAST uses PAC to set up a protected TLS burrow and a succession of TLV to scramble client's verification amid transmission. Figure 2 exhibits how EAP-FAST messages are traded by the supplicant, authenticator, and verification server.

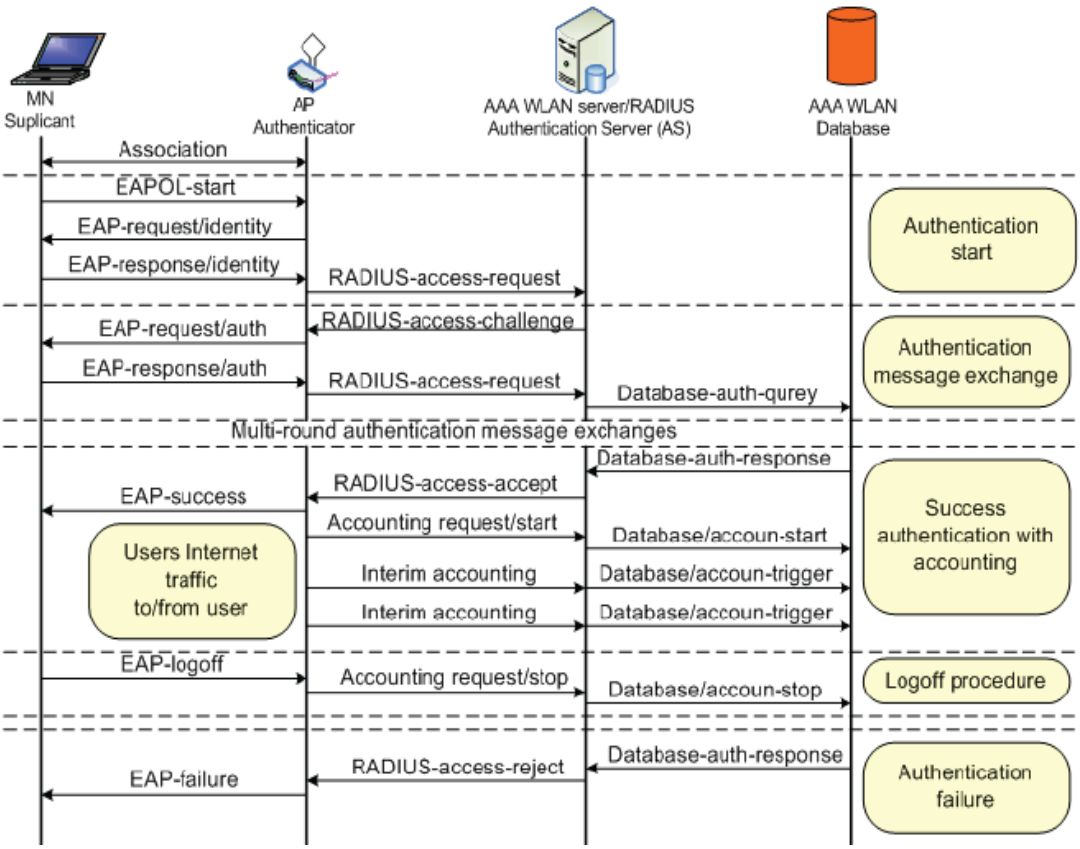


Figure 2 EAP-EAST Messages Exchange for Supplicant, Authenticator (AP) and AS (RADIUS)

1.3 Overview of IEEE 802.1X Authentication Process

The illumination of 802.1X/EAP verification forms that occur between the supplicant programming, the authenticator and the validation server has been depleted in Figure 2. For this procedure to emerge three compulsory procedures must occur to open the controlled port to get to the web. These procedures incorporate; (a) the open framework confirmation (OAS), the 802.1X/EAP process, and the 4-way handshake. The ensuing areas 1.4, 1.5 and 1.6 show these methodologies.

1.4. OAS

In OAS the authenticator (AP) communicate it signals outlines at an interim of like clockwork. On the off chance that the remote customer got the guides outlines, the trading of reaction and demand occur through the un-controlled port has appeared in Figure 3.

The OAS is presently entire starting here, if the system does not have any hostage entrance requesting accreditations then the customer can surf the system. In this point, IEEE 802.1X measures fly in to support the verification component by alarming the confirmation server to close the radio and piece the supplicant from getting to the system until the point when the validation server consents to open the virtual security port. Once the radio correspondence port shuts the IEEE 802.1 X verification, process starts. In this situation, it is obligatory that the OAS the process is required to provoke IEEE 802.1X confirmation process which thusly brings the authenticator

Into play. Figure 4 plots some important strides of 802.1

X/EAP confirmations conspire.[9]

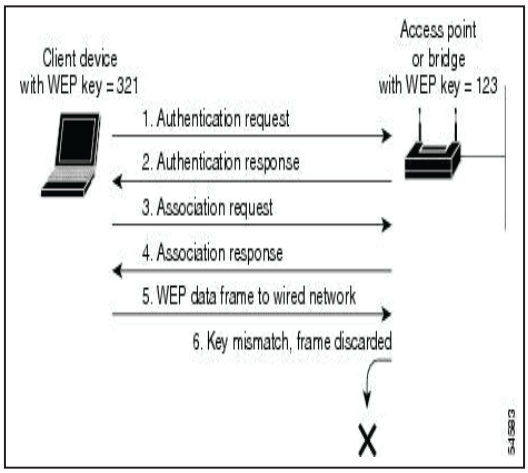


Figure 3 Open Authentication System (OAS)[18]

Once the IEEE 802.1X confirmation is expert, the Master Key (MK) is worked out at AS and the supplicant. This MK will be not scattered to all customers in the whole system. It will be profited to the customer asking for the administration just and already substantiated, and it will be bound to the whole session.

3

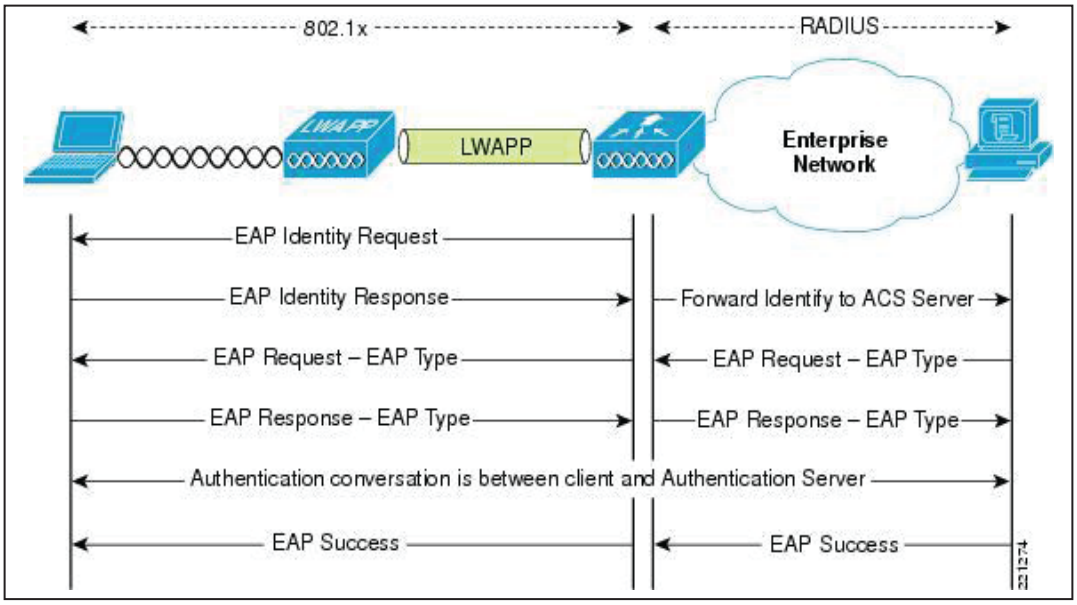


Figure 4 802.1X/EAP Messages Swap[9]

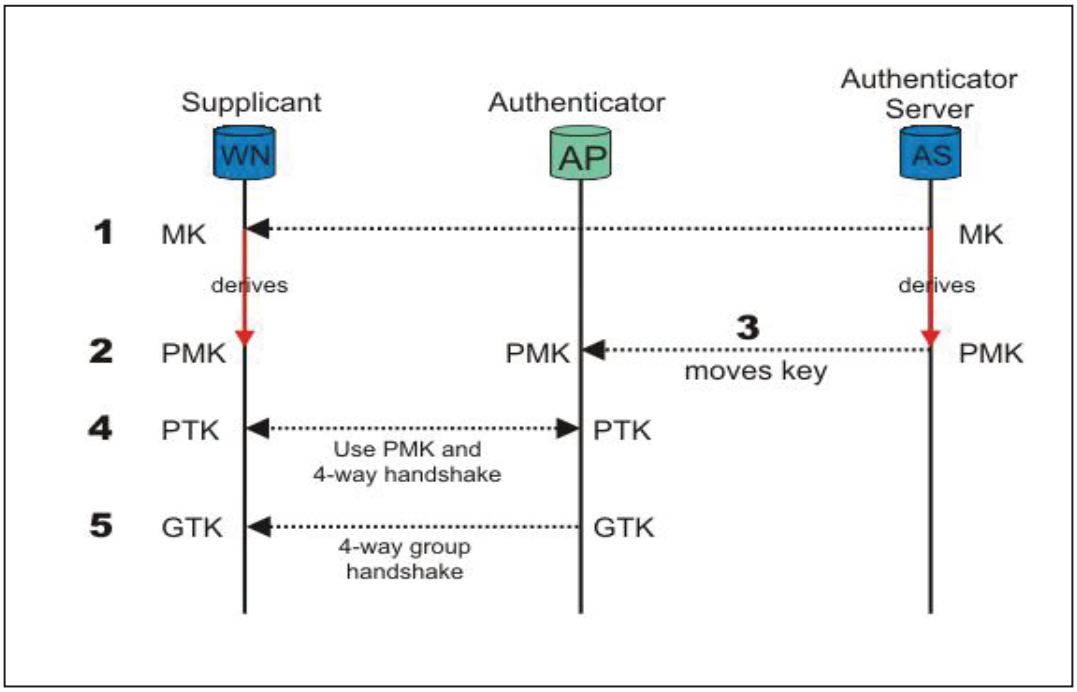


Figure 5: The 4 -Way Handshake Mechanism [9]

The MK key computed up to this point is utilized to create the pairwise ace key (PMK) in favor of the supplicant programming and verification server programming. The AS disperses the PMK to the authenticator in a sharing system.

This PMK produced, will be used in the subsequent method known as the 4-way handshake after a success EAP message. If

the validation is not productive, the process is dismissed and loops back to the OAS state. Figure 5 depicts the four-way handshake tool.

In the above procedure, EAP epitome over LAN (EAPOL) in a general sense transmit EAP outlines from the supplicant to AP specifically by a LAN MAC benefit in four stages as appeared in Figure 5. The supplicant utilizes the once from the Authenticator and PMK to create the pairwise transient key (PTK) to unscramble and encode unicast movement for this session as it were. The PTK isn't shared among the customers yet just between the supplicant and the AP sending an affiliation test. Transmission of this key is by the wired medium framework to the goal hub to counteract sniffing of the key's bundles. On the other hand, the Group-Master Key (GMK) delivered is utilized to figure amass worldly key (GTK) for multicast or communicate circulation inside the managerial space for different customers to acquire a duplicate.

1.5. Three-Party Mechanism

In the above procedure, it can be shown in a three-section situation to rearrange how the messages were exchanged between the gatherings included. In the process the customer (supplicant), the security protects (authenticator) and the supervisor (verification server). The customer wishes to meet the supervisor, and at the passageway, the protection confirms the customer's subtle elements, for example, names by checking the recognizable proof cards. After confirmation and security registration, the protection informs the manager of the customer's landing.

The manager asks from the watch whether an arrangement date was reserved for that specific customer. On the off chance that the arrangement was protected, the supervisor arranges the watch to allow access to the customer. In the event that the arrangement isn't substantial, at that point authorization is denied.

In this situation, the protection does not do anything other than rather just passes the data to the customer and the supervisor. This is identified with the authenticator whose essential obligation is to approve the correspondence between the supplicant and the AS.

1.6. Major Threats to Wireless Network Security

The dangers to systems change as indicated by the need of the assailant. These assaults can be dynamic or detached. Numerous Linux-construct munitions stockpiles are accessible in light of the web as free source codes along these lines cheering assaults to happen to break privacy, trustworthiness, and accessibility

Table 3 beneath condenses a portion of the assaults forced by the dark cap programmers.

Frauds are exploiting remote systems that have not been completely arranged, open confirmation or with powerless security convention gauges utilized. They have outfitted instruments and with programming

that can be downloaded to the web to sniff and catch parcels. They will later investigate the bundles to get more data to assault the system.

Because of this, right security is superlative while conspiring and utilizing an endeavor Wi-Fi arrange.

Attacks Category	Illustration
Man-in-the-Middle (MITM) Attack	Imposter dynamically mimics several authorized parties, such as impersonating to be a client to an AP and vice versa. Allows Imposter to capture communications between authenticator and supplicant, to get valid credentials and information
Misappropriation	Imposter steals or creates unsanctioned use of services
Masquerading	Imposter mimics a legitimate user and achieves certain unauthorized rights and roles
Denial of Service	Imposter averts or limits the usual use or management of the networks and its networks' devices
Message Modification	Imposter modifies a legitimate message by obliterating, adding to, varying or reorganizing it
Traffic Analysis	Imposter passively screens transmission to identify communication designs and partaker s
Eavesdropping	Imposter passively screens the network communications for information, including login details such as passwords and usernames
Message Replay	Imposter passively screens transmissions and retransmits messages, behaving as if the Imposter was an authorized user.

Table 3 Major Threats against Wireless Network Security [19]

2. Related Work

The primary point of security for remote systems is to improve the center standards, for example, accessibility, classification, uprightness and shared validation. Wi-Fi Protected Access 2 (802.11i measures) grasps the utilization of IEEE 802.1X/EAP for confirmation. Then again, information encryption and honesty depends AES - CCMP or AES - Galois Counter Mode Protocol (AES - GCMP) for WIGig systems. Virtual private systems (VPN) and IEEE 802.1X/EAP are broadly conveyed in big business' WLAN to help confirmation and access control notable when arranged with verification, approval, and bookkeeping (AAA (Triple "A")) servers to screen activity and give visitor get to. The present principles, for example, 802.11ac and 802.11ad additionally receive the 802.11i security benchmarks. AAA servers, for example, secure access control server (ACS) to give the inside database to store login certifications for true blue clients.

EAP-FAST is the current IEEE 802.1X/EAP write conveyed generally because of its pick up of tolerating powerless passwords, and computerized endorsements are discretionary as point by point in RFC 4851. This convention encodes EAP execution with transport level security.

(TLS) burrow between the customer and the servers, for example, RADIUS or Diameter. EAP-FAST uses ensured get to certifications (PAC) which store qualifications and information used to monitor the confirmation procedure. Parts of the PAC are figured by the server and are not perceptible to different articles. Customers are anticipated to accumulate PACs locally for use all through confirmation instrument. It is quick that EAP-TLS since it utilizes symmetric

encryption instrument.

Recreation apparatuses, for example, Cisco Packet Tracer, Network Simulator and Huawei's endeavor organize reenactment program (eNSP) are broadly arrange test systems in planning system topology, execution and security in virtual conditions that make it less demanding to embrace it in the genuine condition [13], [14]. Reenactment has been conveyed at the MAC layer to test its execution in regards to handoff to a customer meandering in a vicinity where a few access guides exist utilizing OMNet++ toward decide the inactivity of part exchanges between the entrance focuses and exchange of session keys to ease rekeying qualifications inside the Aps. OPNET a business instrument for Linux has likewise been utilized to configuration secured remote LANs work topology as showed by to assess bundles dropped amid PING between the gadgets inside the system. Recreation is reasonable and furthermore spares time if contrasted with the genuine tested as confirmed by which widely considered different reproduction devices.

Remote security thought is expected to ensure the wired systems. Likewise, VLAN ought to be arranged to permit committed IP subnet as it were. In the event that an assailant tries to unplug the approved gadget and module a rebel gadget, the port will naturally close down, in this way foiling the aggressor from getting to administrations and in addition getting to the systems' setups. The essential VLANs connected in big business/associations are the medium access control based or port-based to set a client to the specific gathering of IP subnet

The ports for switches, validation servers, switches, centers and APs are the focused on ports for playing out the port-based security to accomplish verification and approval as depicted in.

3. Logical Design of the Enterprise Wlan

Figure 6 is a diagrammatical portrayal of the consistent outline for the proposed topology for an association WLAN with six bases. One AP was introduced in each base as appeared in Figure 6 and parameters outlined in Table 4.

The accompanying advances were received to guarantee wandering of customers inside the building was accomplished without detachment of the customers by utilizing a WLC web graphical UI.

1. Construct a comparative standard WLAN on both WLC controllers.

2. Configure comparative portability managerial gatherings on the controllers by exchanging their part MAC

Address and part IP deliver of WLC2 to WLC1 and the other way around. The MAC address and IP Address for WLC2 are 00.1b.d5.69.39.20 and 10.20.1.100 separately while WLC1 are 00.1c.58.89.6c.20 and 10.10.1.100 individually.

3. Confirm virtual interfaces are comparable to the two controllers.

4. Configure Access point 1, 2 and 3 to utilize the controller with benefit port interface 192.168.1.200/24. Additionally 3, 4 and 6 to utilize a similar controller with benefit port administration 192.168.1.201/24.

Floor	AP Label	VLAN Name	VLAN IP Subnet
1st	AP1	VLAN10	10.20.1.100/24
2nd	AP2	VLAN20	20.20.1.100/24
3rd	AP3	VLAN30	30.20.1.100/24
4th	AP4	VLAN40	40.20.1.100/24
5th	AP5	VLAN50	50.20.1.100/24
6th	AP6	VLAN60	60.20.1.100/24

Table 4 Simulation Requirements for logical design of an Enterprise WLAN[random values]

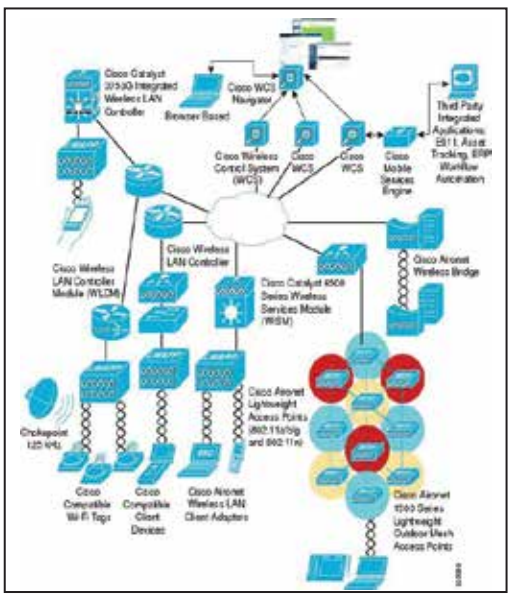


Figure 6 Flat Logical Design of Enterprise WLANs with Six Bases [21]

IEEE in July - 2008, builds upon the IEEE 802.11i safety by given that faster and protected key hierarchy based handoffs in micro seconds when a client travels from current APs to the target AP. IEEE 802.11K is also necessary to permit roaming between different groups for instance from 5GHz to 2.4 GHz.

Strong security can be achieved by configuring WLANs using the Cisco WLC as shown in Figure 6 above. The following operations were performed;

1. A VLAN was created on each floor of the building with a WLAN profile name roaming. Layer 3 policy was configured as web policy for authentication.

2. Configured the WLCs for external web login page by redirecting the login window to a web page to inputs fields for required login details.

3. The RADIUS/LDAP servers' databases were configured to query credentials from Active Directory such as the Cisco Secure ACS server capable of providing Triple "A" services as well as storing the login web page which allows users' credentials interface.

4. The LDAP/RADIUS databases were designed for wireless clients to connect to the internet via a redirection login web page.

3.1. Fast Roaming with Opportunistic Key Caching (OKC)

A few merchants are thinking of a non-standard OKC to diminish handover dormancy for the customer to disassociate the old AP and connect with the objective AP. This sounds great since the 4-way handshake will be skipped. In this procedure, the customers conclude that it is the ideal opportunity for meandering and the AP confirmed to the customer sends the PMK to the objective AP before the customer drops the old AP network. The objective AP and the customer symmetrically ascertain their new PMKs. Upon the re-affiliation, the objective

AP approves the MAC address of the customer sending the demand message. On the off chance that the PMKs coordinate, the customer gets associated. Figure 7 demonstrates a screenshot clarifying how OKC helps in trading cryptographic keys and also giving a protected meandering condition between the customer and the AS.

In Figure 7 Someone is downloading a video utilizing his Tablet PC-PT (versatile hub), and he is on the first Floor and wishes to stroll to where Bob is on the third floor and come back to his office. For any person to proceed with video downloading process, wandering component must be considered amid the outline of WLAN. The bigger circles speak to cell scope for APs A, B and C through the littler circles named X and Y speak to the best coverage areas where wandering happens. For any person to proceed with the video download, the accompanying measure happens

a) OKC advances the PMK of access indicate an entrance point B, which is subject to the WLAN plan and typically activated by WLC or AP itself utilizing restrictive conventions.

b) Before the customer wanders, it quick registers another PMKID by including current AP B's PMK, the objective AP B's MAC address, and the IPAD MAC address.

Supplicant dispatches a re-affiliation ask for the casing to the objective AP B with a novel PMKID.

c) On the other hand, Target AP B breaks down at the MAC address of the IPAD that is sending and a re-affiliation ask for and figures new PMKID utilizing the comparative recipe. The objective AP B answers with a re-affiliation reaction.

d) Here the four-route handshake of 802.1X/EAP has been maintained a strategic distance from and last keys required produced.

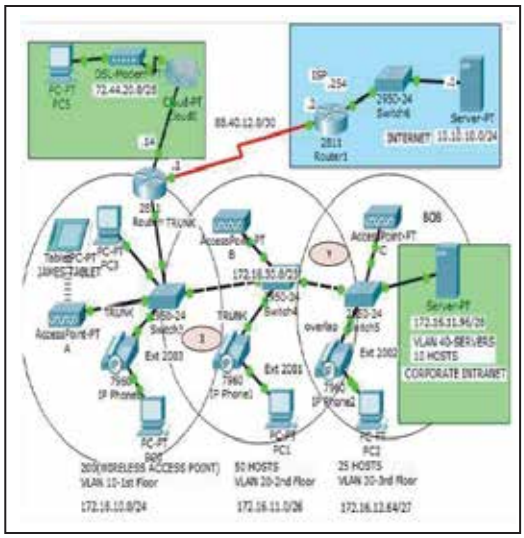


Figure 7 Roaming Description Using OKC[21]

4. Simulation of the Enterprise Wlan

System reenactment is a fundamental component in correspondence building. It encourages architects to create and test organizes execution before sending it in the genuine condition to spare time and in addition limiting the cost. Table 5 demonstrates the reproduction strictures setup.

Floor	VLAN Name	VLAN IP Address	Number of Clients
1st	VLAN1	172.16.10.0/24	50
2nd	VLAN2	172.16.11.0/26	50
3rd	VLAN3	172.16.11.64/27	50
4th	VLAN4	172.16.11.128/29	50
5th	VLAN5	172.16.11.160/30	50
6th	VLAN6	172.16.11.192/31	50
Intranet Parameters			
	VLAN Name	VLAN IP Address	Number of Host
Internet	VLAN80	176.16.11.96/28	10

Table 5 Simulation Parameters [random values]

Figure 8 below shows the screenshot of the simulated parameters using Cisco Packet Tracer (CPT). CPT is a powerful tool developed for simulating both LAN and Wi-Fi topologies.

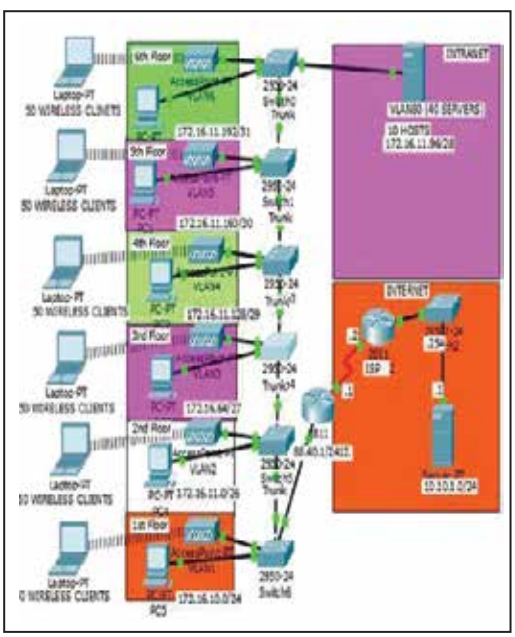


Figure 8 Simulation of the Proposed Enterprise Wi-Fi[21]

In this situation, six APs were sent to make the VLAN per each floor for pragmatic purposes. On the intranet side, the Cisco Secure Access Control Server was utilized to give triples "An" administrations. In this server, an establishment of RADIUS and LDAP databases was performed to give customers' login points of interest. In every customer's PC, a VPN programming was introduced to give a VPN secure passage between the APs and the VLAN. An 802.1X/EAP was empowered to set up a safe RADIUS burrow between the authenticator and the supplicant for messages movement.

Clients who meander from the sixth floor to the first floor uses layer two wandering for VLANs associated with one WLC and layer three meandering for VLANs associated with various WLCs. At the point when clients meander inside the remote system cell, their IP addresses stay unaltered though WLCs disperse the qualifications to the accessible APs. The trust relationship assertion between the WLCs ought to be made to guarantee that the correspondence doesn't interfere. In any case, zero bundles misfortune is difficult to anticipate amid the handoffs system. The qualifications stayed unaltered all through the wandering procedure, hereafter guaranteeing portability and secure passage inside the system to restrain disavowal of-benefit assaults and essential recovery of the key amid the 4-way handshake strategy.

When outlining a WLAN by reenactment process, the accompanying meandering rules ought to be taken after to enhance the general system execution;

- An AP can just trade data with customer gadgets that help its remote convention gauges.

- All APs should have the indistinguishable system name to help customer meandering.
- All APs and the supplicants ought to have a closely resembling security setting to impart.
- All APs in the comparative position must make utilization of an unmistakable and self-sufficient channel.
- APs that utilization a similar channel ought to be introduced as far from each different as conceivable to stay away from or diminish potential obstruction.
- The APs' scope cell ought to overlie at a level of 15 to 25 to ensure that there are no gaps in the scope territory to guarantee that the meandering customer will dependably have an all-inclusive purpose of handoff that is predefined.

4.1. Mobility Simulation Using NS2

In this test, two APs and one portable station were intended for reproduction purposes by NS-2 Tcl content which is mainly a protest arranged interpreter. AP1 was put at x=200 and y=100 organizes. AP2 is set at x = 600 and y=700 arranges. The customer was related to AP1 at directions of (x=200 and y=150). Dynamic source directing convention was utilized [26] since it is on request steering convention. The customer meanders from AP1 to AP2 and stops at facilitates (x=600 and y=500) to be related to AP2. This reproduction was rehashed for ten times by changing the source and goal facilitates and the outcomes acquired are appeared in Table 6. These outcomes were examinable utilizing the tracegraphv202 graphical UI to break down the system data.

Serial Number	Full-Authentication average(seconds)	Handoff Speed (Seconds)
1	5.5	0
2	0.62	0.041
3	0.87	0.052
4	0.83	0.012
5	0.85	0.058
6	0.91	0.03
7	1.2	0.05
8	0.71	0.033
9	1.04	0.021
10	1.12	0.018

Table 6 Full 802.1X/EAP Authentication and Handoff Speed In the above investigation, serial number 1 with an aftereffect of 5.5 seconds shows the full-verification process though serial numbers 2 - 10 demonstrates the re-confirmation forms.[11]

5. Results and Discussion

In this area, the mimicked comes about are examined and broke down. For viable purposes, 6 APs are settled to cover a six-story condo. All APs are connected to a spine IP Network, to where a RADIUS server, dynamic host setup convention (DHCP) server, area name framework (DNS) server are name framework.

(DNS) servers are likewise connected. DHCP server performs programmed circulation of IP delivers to all gadgets associated with the system utilizing DHCP Pool. Initial, a thought of the handover speed and full verification incite for three models as delineated in Table 7. The reasonable recreation consequence of and

for EAP-TLS and EAP-ESIM full confirmation was utilized to contrast EAP-FAST verification technique with demonstrate its viability in regards to handoff speed.

Authentication / EAP	Full-authentication average Speed in seconds	Handoff speed average (seconds)
EAP-TLS	1.1	0.083
EAP - ESIM	0.876	0.039
EAP-FAST	0.815	0.035

Table 7 Full-Authentication and Handoff Speed Averages for EAP (TLS, ESIM and FAST)

An aftereffect of EAP-FAST full confirmation speed of (0.815 seconds) was gotten utilizing Network Simulator Version 2 (NS2) which is lower when contrasted with the beforehand sealed consequence of 1.1seconds and 0.876 seconds in the writing of and individually. These outcomes can be lower than the found the middle value of dormancy time when tried in the genuine processing condition. Idleness time is decreased by guaranteeing that an officially settled shared security enter in the current AP is moved to the closest target AP to lessen inactivity. This is finished by the utilization of OKC where the PMK is moved to the focused on AP before re-relationship of the customer happens. OKC PMK reserving empowered quick handoff in Wi-Fi systems since the PMK identifier made amid full verification is disseminated to the whole APs through the AS. At the point when the customer triggers the wandering procedure, it quick processes the PMKID2 utilizing the first PMKID1. Then again, the AP registers the PMKID2 utilizing the first key send by the past AP. Amid affiliation, the objective AP just checks the MAC address of the customer and approves the key. EAP-FAST will be quick however not as secure as EAP-TLS. It is suggested that the inactivity ought to be under 150msec (0.15sec) to help VoIP and video parcels transmissions as portrayed. This suggests the inertness must be generally low. In the reenactment analyze, it clear that EAP-FAST accelerate the handoff procedure to give client's portability consistently. Portability was to accomplish by making a put stock in relationship amid the outline of the remote system. In Figure 7, the supplicant does not believe the authenticators in VLAN20 and VLAN30 for setting data exchange. This issue was illuminated by putting WLCs as appeared in Figure 6 to wipe out superfluous re-validation. In VLAN80, a few servers are accessible for different purposes. For example, a social trust by means of shared mystery key exists amongst AS and AP, the understood put stock in coincide between the supplicant and the AP and trust by means of EAP-FAST co-happen between the AS and the supplicant. Range server works in this plan was to appropriate shared mystery keys in front of the customer by means of RADIUS burrow. A verge plane of 25% ought to be utilized to enable the customer to settle on the meandering choice when the flag to commotion proportion turns out to be low contrasted with the edge. Remote channel portion is likewise crucial. Contiguous APs must have a distinction of five diverts in the middle of them to evade direct impedance as portrayed in Figure 7. In basic, Access Point-PT an ought to be allotted channel one and Access Point-PT B ought to be allocated channel six. In handoff process, AP disclosure (examining) constituents around 90% of the wandering inactivity as outlined. In the new plan received in this article, AP filtering process was wiped out after an 802.1X/EAP full confirmation strategy. Along these lines EAP-FAST lessens the full confirmation

normal by 26% when contrasted with EAP-TLS and 7% when contrasted with EAP-SIM. Then again, EAP-FAST handoff speed was likewise decreased by 58% when contrasted with EAP-TLS and 10% when contrasted with EAP-SIM. The EAP-FAST confirmation convention is the most proper to be sent in a remote undertaking condition.

6. Conclusion

In this research, an association WLAN which conveyed IEEE 802.1X using EAP-FAST that does not require authentications, was created. EAP-FAST lethargy which is insignificant in contrast to EAP-TLS and EAP-ESIM was illustrated. EAP-FAST uses the symmetric cryptographic keys which diminish inertness. The primary element of Wi-Fi organizer is secure wandering without rekeying of usernames and secret word. However, providing login certifications to the client for speedier validation creates disturbance for administrators. One such example is video gushing or voice calls. In spite of the fact that EAP-FAST is the innovation from Cisco, it is still subjected to a MITM assault and if enough parcels are caught, at one point it is conceivable to mount a word reference assault. This is accomplished by ensuring the WLCs have been designed to exchange cryptographic keys from the current AP to the new AP before the affiliation and the goal is a two-way handclasp that is utilized rather than the 4-way handclasp, which involves various messages swap. A WLAN with a few VLANs was produced to cover the six stories of the working to upgrade handoff velocities to lessen idleness. Customer's machine is equipped with VPN to reinforce encryption. ENSP and CTP programs gave parts that speak to the physical gadgets, which permit working with various system gadgets in a virtual system. Similar to this is a more valuable work to be done in light of the fact that no time squandered is acquired on the off chance that it was done in the research facility where cabling establishments are obligatory to interface different remote components with various network topologies.

In the reproduction, no much cost is required while setting up the virtual condition aside from insignificant causes when obtaining some business organize test systems if the need emerges.

Later on, a broad research ought to be finished with a desire of building up an EAP compose that is secure and supersedes wandering dormancy and word reference assaults forced by the MITM assaults to scale-up the framework execution and in addition enhancing security. Graphical UI (GUI) test systems should be produced to consolidate every one of the gadgets utilized as a part of remote systems, for example, WLC whose symbols are not accessible in different system test systems and emulators to limb the realness of reenactment.

7. References

[1] B. R. Nishanth, B. Ramakrishnan, and M. Selvi, “Improved Signcryption Algorithm for Information Security in Networks,” Int. J. Comput. Networks Appl., vol. 2, no. 3, pp. 151–157, 2015.

[2] P. Mittal, “Implementation of a Novel Protocol for Coordination of Nodes in Manet,” Int. J. Comput. Networks Appl., vol. 2, no. 2, pp. 99– 105, 2015.

[3] T. Jeffree, P. Congdon, and M. Seaman, IEEE Standard for Local and

Metropolitan area networks - Port-Based network Access Control, Revision o. New York, USA: IEEE Computer Society, 2010.

[4] E. Tews and M. Beck, "Practical attacks against WEP and WPA," Proc. Second ACM Conf. Wirel. Netw. Secur. - WiSec '09, pp. 79–83, 2009.

[5] U. Kumar and S. Gambhir, "A Literature Review of Security Threats to Wireless Networks," Inernational J. Futur. Gener. Commun. Netw., vol. 7, no. 4, pp. 25–34, 2014.

[6] A. Chiornita, L. Gheorghe, and D. Rosner, "A practical analysis of EAP authentication methods," 9th RoEduNet IEEE Int. Conf., pp. 31–35, 2010.

[7] Q. Qiongfen and L. Chunlin, "On Authentication System Based on 802.1X Protocol in LAN," pp. 2–5, 2010.

[8] J. Lázaro, A. Astarloa, U. Bidarte, J. Jiménez, and A. Zuloaga, "AES-Galois Counter Mode Encryption/Decryption FPGA Core for Industrial and Residential Gigabit Ethernet Communications," in Proceedings of the 5th International Workshop on Reconfigurable Computing: Architectures, Tools and Applications, 2009, pp. 312–317.

[9] W. Alliance, "The State of Wi-Fi ® Security," no. January, pp. 3–15, 2012.

[10] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 184– 208, 2016.S. Zafar, "Throughput and Delay Analysis of AODV , DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks," *Int. J. Comput. Networks Appl.*, vol. 3, no. 2, pp. 25–31, 2016.

[11] S. Sotillo, "Extensible Authentication Protocol (EAP) Security Issues," *Syst. Technol. East Carolina Univ.*, pp. 1–6, 2007.

[12] J. Salowey, N. Cam-Winget, D. McGrew, and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST) Status," *Cisco Syst.*, pp. 1–64, 2007.

[13] S. M. Hashimi and A. Güneş, "Performance Evaluation of a Network Using Simulation Tools or Packet Tracer," *IOSR J. Comput. Eng.*, vol. 19, no. 1, pp. 01–05, 2017.

[14] G. F. Riley, "Using Networks Simulation in Classroom Education," *Proceeding 2012 Winter Simul. Conf.*, pp. 2837–2841, 2012.

[15] A. Nayyar and R. Singh, "A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs)," *J. Wirel. Netw. Commun.*, vol. 5, no. 1, pp. 19–47, 2015.

[16] B. Aslam, M. Akhlaq, and S. A. Khan, "IEEE 802 . 11 Wireless Network Simulator Using Verilog," *Proc. 11th WSEAS Int. Conf. Commun.*, vol. 2, pp. 393–398, 2007.

[17] M. H. Noshy and A. Z. Mahmoud, "Performance Comparison between

LTE and WiMAX Based on Link Level Simulation," *Int. J. Comput. Networks Appl.*, vol. 4, no. 5, pp. 121–128, 2017.

[18] J. Pan and R. Jain, "A survey of network simulation tools: Current status and future developments," *Washingt. Univ. St. Louis, Tech. Rep*, pp. 1– 13, 2008.

[19] S. T. Chandel and S. Sharma, "Performance Evaluation of IPv4 and IPv6 Routing Protocols on Wired, Wireless and Hybrid Networks," *Int. J. Comput. Networks Appl.*, vol. 3, no. 3, p. 59, 2016.

[20] OKC http://support.huawei.com/enterprise/en/network-management/ensp-pid-9017384/software

Alyas *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

Advanced User Interfaces from iOS To Windows 8

Syeda Binish Zahra[1], Syed M. Shabih-Ul-Hassan[2]

[1]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan.

[2]Professional Academy of Commerce, Lahore, Pakistan
binishzahra@lgu.edu.pk[1] shabih@pac.edu.pk[2]

Abstract:

This article discusses porting advanced user interface features from an iOS app to a Windows Store app. We use an electronic medical record (EMR) application for this case study. This paper can give new direction for windows 8 to windows 10 porting.

Keywords: Hypertext Markup Language (HTML), integrated development environment (IDE), User-Interface (UI).

1. Introduction

In recent years, tablets, as new forms of mobile computing platforms, have quickly moved from the consumer electronics spaces into the business and enterprise computing domains. After the release of Windows 8 operating systems earlier this year, we felt there was a need to provide some quick start tutorials for developers on how to port their existing apps from other platforms such as iOS to Windows 8, and start developing new apps on Intel UltrabookTM devices, tablets, and other Intel architecture-based devices running Windows 8. This article serves this objective and focuses on the advanced user interface topics.

On iOS, natively Objective-C is the main development language. For Windows Store apps, you have multiple choices available, including Visual C#, HTML / JavaScript*, and others. In this case study, we use Visual C#* as the development language of choice.

2. From Xcode* 4 to Visual Studio* 2012

Like the Xcode tools package on OS X* for iOS application developers, Visual Studio 2012 provides an integrated development environment (IDE) for Windows Store app developers [2]. Also like the Interface Building design tool on Xcode 4, which supports storyboarding (Figure 1), Visual Studio 2012 includes a XAML Designer tool (Figure 2).

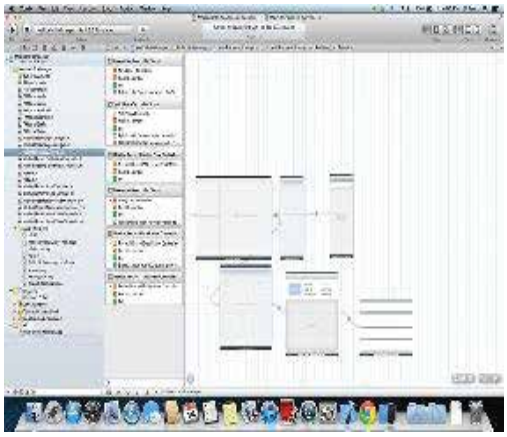


Figure.1: The Interface Builder in Xcode 4

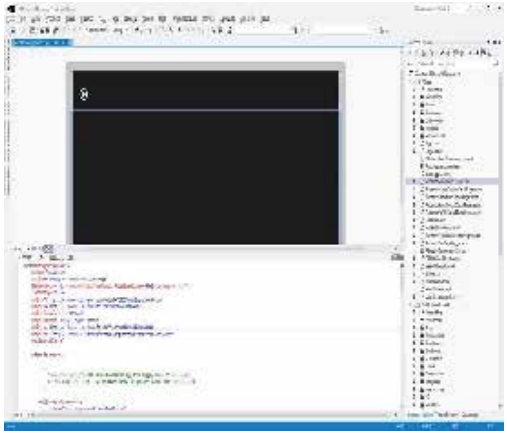


Figure.2: Visual Studio 2012 XAML Designer

3. The Case Study Project

This article is one of a series based on a case study project. In the project (link to the folder of other articles based on this project), we ported a medical record management application from iOS to Windows 8. The basic requirements of the application include:

- Show a list of patients
- Show the personal and medical information of a specific patient, which includes identity, billing, vitals, lab tests, medical images, etc.
- Display detailed graphs and images when selected

This article will cover the advanced UI features of the project.

4. High Level UI Design and Navigation Patterns

On iOS, we can use the split-view controller to present a master view and a detailed view on the screen. We can use table views or tab bar views to group different categories of information on the view. Figure 3 shows the split view along with the master table view and the detailed table view [3]. The left pane of the split view shows the scrollable patient list. The right pane shows the medical records associated with the selected patient in the list. We use a table view to put the medical record categories on the same view. We can also use the tab bar view, with each tab view displaying a specific medical record category. Figure 4 shows how this view is created in Xcode 4 storyboard.

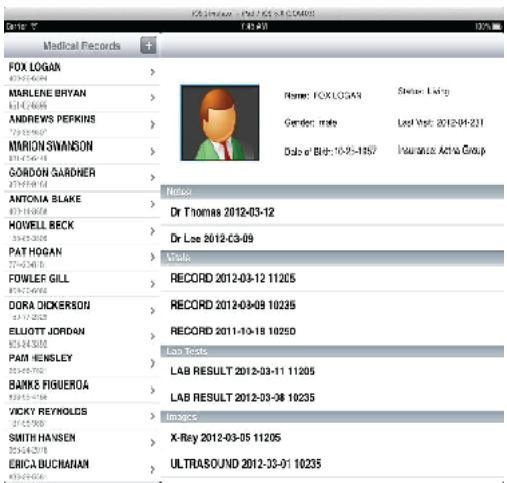


Figure.3: On Ios, A Split View Controller And Its Master Table View And Detailed Table View

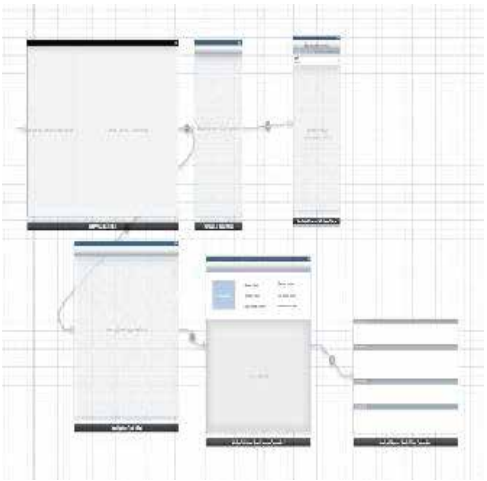


Figure.4: Use Xcode storyboard to create a split view and its master and detailed table views

In a Windows Store app, we can accommodate this design by following the Windows Store app hierarchical system of navigation pattern (Figure 5). The first level page shows a grid view that includes a tile for each patient (Figure 6). The second level page is a grouped item page that includes the medical records for the patient selected from the first level page (Figure 7). The third level page is a group detail page that shows the specific category of medical records selected from the second level page (Figure 8). We can also have a fourth level page that shows the item details, for example, the actual X-ray image selected from the third level page.

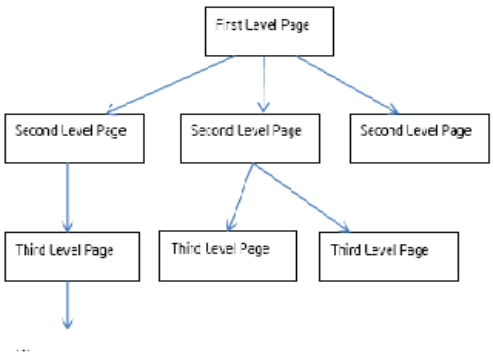


Figure.5: Windows Store app hierarchical system of navigation.

Figure.6: In the Windows Store app, the root level grid view includes tiles for the patient list.

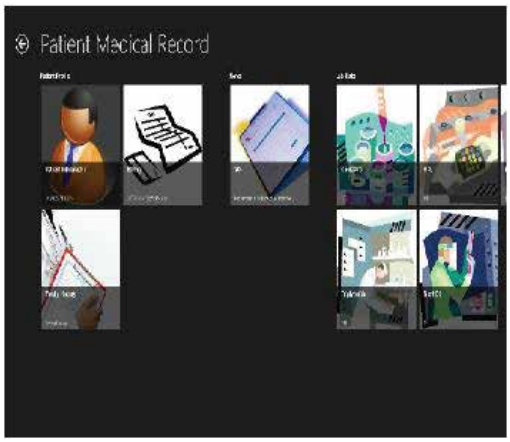


Figure.7: In the Windows Store app, the second level page shows the medical records associated with the selected patient.

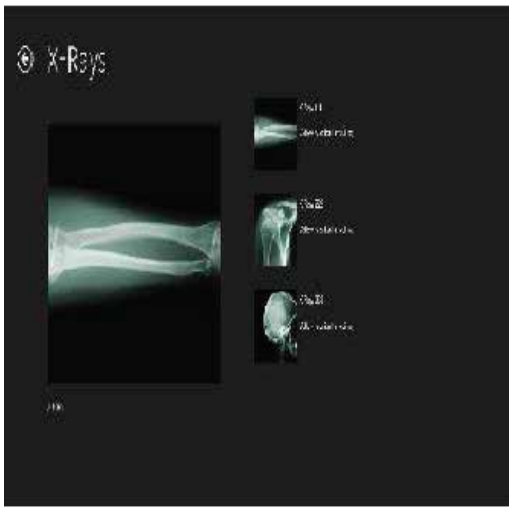


Figure.8: In the Windows Store app, the third level page shows the group selected from the second level page.

Visual Studio 2012 projects, the UI page is defined with a "XAML" file and a C #implementation file (.cs) associated with it. Because the transitions from one page to another page usually originate from user actions, for example, when a grid view item is pressed, naturally the event listeners are the places used to handle the navigations.

5. Windows Project Templates and Data Binding

In Figure 7 and Figure 8, items are grouped and shown nicely in the grid views. Visual Studio 2012 Windows Store project templates provide a powerful basis to construct these user interface pages. The predefined project templates include grouped items page, group detail page, item detail page, etc. We use the X-rays group detail page as an example here.

In Visual Studio 2012's Solution Explorer window, right click the project name and select "Add -> New Item…" from the pop-up menu. Select "Visual C#" on the left pane. On the center pane, we see the list of the predefined page templates. Among those templates, we select "Group Item Page." A preview of the template is shown on the right pane. We also enter a name for the page in the text box at the bottom of the dialog (Figure 9), and press the "Add" button. Visual Studio 2012 now generates a file named "XRayImagesGroup DetailPage.xaml" file and a file named "XRayImagesGroupDetailPage.xaml.cs" in the project.

Figure.9: Add New Item dialog shows the Window Store project templates (**)

In Visual Studio 2012, if we expand the "Common" folder generated under the project (Figure 10), we can see Visual Studio has generated a group of files under it. Among these files, LayoutAwarePage.cs contains the class that we derive the XRay Images GroupDetail Page from.

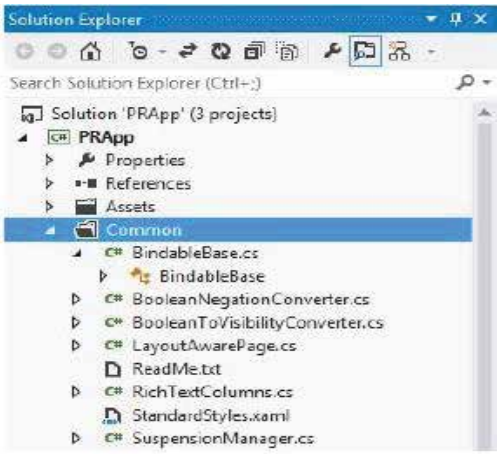


Figure.10: The "Common" folder in the project.

The “Common” folder also includes the “BindableBase.cs” file. We derive a data model for the view from this class.

6. Conclusion

Advanced user interface with IOS are more helpful and secure when we compare its functionality and performance with windows OS. The case study of electronic medical record (EMR)is showing the reliability of advanced user interface we add or modify some features of IOS ,then this operating system will become more reliable than any operating system that are used in market.

7. References

1. Heuristic evaluation- Nielsen, Jakob. Useit. How to conduct a heuristic evaluation. http://www.useit.com/papers/heuristic/heuristic_evaluation.html (Retrieved 2011-05-19)

2. Kumar, Minu, and Garg, Nitika. Aesthetic principles and cognitive emotion appraisals: How much of the beauty lies in the eye of the beholder? Journal of Consumer Psychology. Vol. 20, No. 4. (October 2010) E-Journals, EBSCOhost (Retrieved 2011-05-18)

3. Kurki, Ilmari, and Repokari, Lauri, and Saarela, Toni. Visual search on a mobile phone display. SAICSIT '02. (2002):253-253.

Editorial Policy and Guidelines for Authors

IJECI is an open access, peer reviewed quarterly Journal published by LGU Society of Computer Sciences. The Journal publishes original research articles and high quality review papers covering all aspects of Computer Science and Technology.

The following note set out some general editorial principles. A more detailed style document can be download at www.research.lgu.edu.pk is available. All queries regarding publications should be addressed to editor at email IJECI@lgu.edu.pk. The document must be in word format, other format like pdf or any other shall not be accepted. The format of paper should be as follows:

- Title of the study (center aligned, font size 14)
- Full name of author(s) (center aligned, font size 10)
- Name of Department
- Name of Institution
- Corresponding author email address.
- Abstract
- Keywords
- Introduction
- Literature Review
- Theoretical Model/Framework and Methodology
- Data analysis/Implementation/Simulation
- Results/ Discussion and Conclusion
- References.

Heading and sub-heading should be differentiated by numbering sequences like, 1. HEADING (Bold, Capitals) 1.1 Subheading (Italic, bold) etc. The article must be typed in Times New Roman with 12 font size 1.5 space, and should have margin 1 inches on the left and right. Length of paper should not be longer than 15 pages, including figures, tables, exhibits and bibliography. Table must have standard caption at the top while figures below with. Figure and table should be in continues numbering. Citation must be in according to the IEEE 2006 style

LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: ijeci@lgu.edu.pk

Published by: Digital Forensics Research and Service Center , Lahore Garrison University