International Journal of Security and Its Applications
Vol. 12, No. 3 (2018), pp.19-28
http://dx.doi.org/10.14257/ijsia.2018.12.3.03

Practical Guidelines for Securing Wireless Local Area Networks (WLANs)

Ahmed Khan[1] and Aaliya Sarfaraz[2]

[1,2]*Department of Computer Science*
[1,2]*COMSATS Institute of Information Technology, Islamabad, Pakistan*
[1]*ahmed.khan@comsats.edu.pk*, [2]*aaliya.sarfaraz@comsats.edu.pk*

Abstract

The publication generally focuses on the security configuration and monitoring of wireless local area networks (WLANs) which are extensively being used by various organizations. Wireless Local Area Networks (WLANs) presents an exceptional challenge for the different organizations that are using Wireless Local Area Networks [1]. Over the years, the percentage of attacks on Wireless Local Area Networks has been increased, which as a result has compelled the organizations and users of WLAN to rethink about their WLAN security. The publication is a way forward for improving the standards of security and monitoring of the wireless local area networks (WLANs) and the devices which connect to those networks by giving pertinent recommendations. The article is really helpful for all those who are associated with the planning, implementation, maintenance and monitoring of the security of the wireless local area networks of a particular organization and all the devices that are connected to these WLAN like network professionals, security professionals, system administrators and all other entities related with the security of an organization's network. The scope of the publication is restricted to wireless networks that are unclassified and also the unclassified facilities that fall within range of such wireless networks.

Keywords: *Network security, WLAN, monitoring and security standards*

1. Introduction

A computer network generally consists of two or more computers that are connected to exchange data. The computer networks enable the connected devices in sharing of resources like printers and CDs, exchanging files and allowing electronic communications. The computers on a network are usually linked through cables (commonly known as Ethernet), wirelessly (through radio waves), satellites, telephone lines. [2]. In computer networks, network nodes are the devices that originate, route and terminate the data. Generally, the hosts such as phones, servers, personal computers as well as networking hardware can be termed as nodes [3]. Any two devices can be considered to be networked together when one of the devices is able to exchange information with the other device. A computer network can also be termed as a multipurpose connection, which enables a single computer to perform various functions. Common examples of computer networks may be banking networks in which a bank card can be used at an Automatic Teller Machine (ATM) over a large area and message networks that enable people to send and receive mail electronically while using computers [4-5].

There are various types of computer networks. The size of a network can be articulated by the geographic area occupied by the network and the number of devices that form part of the network. Computer networks can cover anything from a small number of devices

Received (January 18, 2018), Review Result (March 13, 2018), Accepted (April 9, 2018)

ISSN: 1738-9976 IJSIA

within a single room to millions of devices spread across the entire globe. On the basis of geographic area, a computer network can be divided into various types, namely Personal area network (PAN), Local area network (LAN), Metropolitan area network (MAN) and Wide area network (WAN). A personal area network (PAN), is generally a computer network which is organized around an individual person within a single building. The building could be a small office or residence. A local area network (LAN) is comprised of a computer network placed on a single site, such as an individual office building. A local area network can be built with relatively inexpensive hardware and is generally very useful in sharing of resources, which can include data storage and printers. A metropolitan area network (MAN), consists of a computer network which spans over a small region, an entire city or a college campus. A metropolitan area network (MAN) is larger than a local area network (LAN) which is typically limited to a single site. A wide area network (WAN) generally covers a very large area, which may include an entire country or the entire world. A wide area network (WAN) can contain multiple smaller networks, including a number of local area networks (LANs) or metropolitan area network (MANs). The most well known example of a wide area network is an internet [6-7].

A wireless local area network (WLAN) is a wireless computer network that connects two or more devices within a specified area such as a home, school, computer laboratory, or office building through radio communication, enabling its users to walk around freely within the area of its coverage and remains connected to the network at the same time, and can provide a connection to the wider Internet. The technology of WLAN mainly rests on the IEEE 802.11 standard and its improvements. The WLAN fundamental components are mainly the client devices which include computer systems, smart phones, laptops and Access points (APs), which are responsible for connecting client devices with an organization's wired network infrastructure. In some cases to act as mediators between APs and the distribution system, wireless switches are also used by WLANs. The dependence of WLAN security lies primarily on the fact that WLAN components, including client devices, access points, and wireless switches are secured throughout from initial WLAN design and deployment through ongoing maintenance and monitoring (the complete WLAN life cycle). WLANs are unfortunately considered less secure than the their wired counterparts for a number of reasons, mainly the simplicity in accessing the WLAN and the loopholes in security configurations which are often used for WLANs to prefer ease of access, resultantly compromising the security aspect [8-10]. The main focus And the prime aim of this publication is to assist the organizations in improving of their security standards of the WLAN by proposing viable suggestions for monitoring and

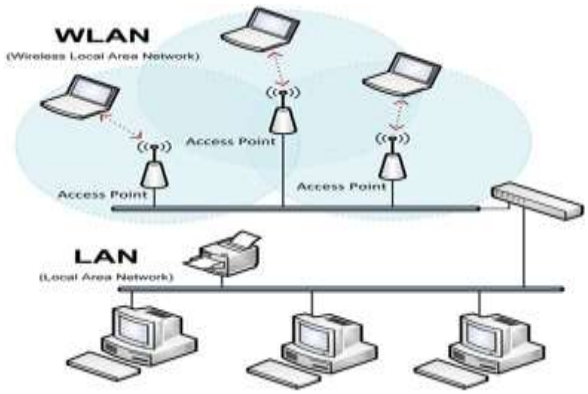

Figure 1. WLAN and LAN Configuration

configuration of WLAN security. The current publication also enhances the other NIST publications related to the field of the WLAN by combining and strengthening their main recommendations. Organizations in order to improve the security of their WLANs should

implement the following guidelines: Impact of successful attacks and vulnerabilities are lessened to a greater degree if standardized configuration is used as a base level of security. Such standardized configurations can also considerably lessen the time and endeavor which are generally required to secure various components of WLAN and in verification of their security [11-14], predominantly in the scenario where automated means are utilized in the deploying and verification of the configuration as above in Figure 1.

A WLAN may be connected to another WLAN or in other case it will be generally connected to a wired network of a particular organization. For those WLANs that need access to a wired network, then the client devices of that particular WLAN should be allowed to access only the necessary hosts by utilizing essential protocols on the wired network. Moreover, in case an organization has a security profile of more than one for WLAN usage, then that particular organization should cater for separate WLANs; for example, an organization should have logically separated WLANs for guests (external use) and for its own workers/users (internal use). The Devices that connect to a particular WLAN should not be able to access the devices on a WLAN which is separated from the first one [15-20].

"Dual connected" means a client device which is connected to a WLAN and a wired network and can access them simultaneously. If an attacker who gets unauthorized access to a device that is dual connected, then that particular user is in a position to attack and access wired network resources [22]. In addition, the organizations should also consider the other forms of threats that evolve as a result of involving multiple wireless networks rather than catering and focusing on the threats that emerge due to dual connections. Nowadays, it has become very regular from various client devices to access various wireless networks at the same time, such as Bluetooth, WiMAX, cell phone and WLAN networks. Organizations should make an effort to evaluate the hazard of various network technologies for their client devices of WLAN and should also find a way out in lessening those particular risks [23]. Dual connections involving a network whose risk is not up to the acceptable level will definitely pose a threat to that particular organization and efforts should be made to prohibit it. After designing security configurations of a WLAN for various Access points and client devices, an organization should focus on the implementation phase of the particular configurations, the usefulness of the those implementations, deployment of the implementations for the suitable devices and maintenance of the configurations [24]. Standardization, automation and centralization of an organization's WLAN security configuration, its implementation and maintenance, is of foremost importance. This enables the organizations to execute reliable WLAN security all the way through the enterprise. Resultantly, detection and correction of unauthorized/ unlawful changes to configurations, and reacting swiftly in case of identification of new vulnerabilities will specify the need to change the security configuration of WLAN [25]. Security monitoring has its own importance in the field of security and it relates to all the networks, but due to the increase in the risks and threats posed to WLAN networks, it is given more weightage in case of networks using WLAN. Organizations should generally make an endeavor to formulate ways for continuous monitoring of their WLANs, which includes wired network and WLAN-specific attacks. Organizations should set the same perimeters and criteria for vulnerability monitoring for WLAN components that they use in case of any other software which includes identification of patches and their application, verification of settings of security configurations and their adjustment as per the requirement. These desired actions should be carried out as frequently for components of WLAN as they are carried out for the organization's wired networks. These assessments if not on a six monthly basis should be executed on an annual basis to assess WLAN security and finding out vulnerabilities to fix them. Furthermore, the organizations should also focus on the periodic assessments which are recommended to be done on a quarterly basis unless and until the continuous

monitoring of security of WLAN is collecting the required data regarding the attacks pertaining to WLAN and the weaknesses required for the evaluation purposes.

In our proposed scheme, the comparative analysis of various attacks and monitoring tools is to be written which describes the vulnerability level to our systems.

2. WLAN Security Monitoring

2.1. WLAN Security Monitoring Basics

The importance of security monitoring is linked to all the networks and systems, but it is normally given importance and attention in case of WLANs. Security objectives of the WLANs and wired networks are generally similar and usually both face same type of common threats, however the security of WLAN is normally difficult to achieve for a number of reasons. Firstly, the WLAN networks are generally easier to access for the attackers than the networks that are wired. The most considerable distinction between the protection of wired and WLANs networks is the fact that wireless network transmissions can be intercepted and fresh and changed transmissions can be sent which is supposed to be from the legitimate source. On the other hand, for monitoring of traffic on wired network traffic, a malicious user has either to access the network physically or has to compromise network systems remotely. However, in case of networks using WLANs, an unauthorized user merely needs to be in the range the transmissions. In some cases, highly sensitive directional antennas are used by the attackers to extend the effective range of attack which is beyond the standard WLAN range.

Secondly, security of WLAN networks is usually not given due importance and are poorly secured in most of the cases. For example, in many cases configuration of WLANs is done in such a way that they do not need tough authentication, resultantly it is very convenient for the malicious users to exploit and effectively gain access to the WLAN. The reason why such configurations are generally used because they are more suitable for both the administrators and the users, but as a result, they often put the devices connected to WLAN and the information being transmitted at serious risk of compromise.

Thirdly, in most of the cases the WLANs are generally connected to a wired network of an organization. Therefore, the organization in this scenario has to counter for the attacks which are specific and related to WLAN but also have to worry about all the attacks that are being faced by the wired networks. Therefore, in order to maintain and augment security of WLAN, the organizations should focus on both the aspects of monitoring which includes attack monitoring and vulnerability monitoring.

2.2. Attack Monitoring

Organizations should make an effort for continuous monitoring of their WLANs including wired network and WLAN attacks. The wired network attacks generally involve the security controls that are being utilized for any system in the network. The attacks related to WLANs in general can be distributed into two key types: passive and active. The various classes of attacks, which are considerable for the purpose of monitoring, are as under:

Passive attack: is a type of attack in which an unauthorized party or an attacker only monitors/ listens to the WLAN communications, the attacker does not change, generate or disrupt WLAN communications. The passive attacks are of two types. Eavesdropping in which the attacker is only interested in the message content and Traffic analysis by monitoring of data transmissions which is also known as traffic flow analysis. The attacker monitors the transmissions for knowing the patterns of communication and gain intelligence. Generally, when two parties are communicating, then a significant quantity of information is present in the messages flow between the parties involved in the communication.

Active attack: is an attack in which malicious user or an attacker alters, generates, or disrupts WLAN communications. Such attacks can be divided into the following types:

Masquerading or spoofing: is impersonation of one entity by another. It lures the victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer while using the internet and reaches another computer then the user has been spoofed. Similarly, if a user intends to read a file and the attacker or an unauthorized user has already planned to give another file to the user then another spoof has taken place.

Replay: is the retransmission of the message by a malicious user or an attacker who is monitoring transmissions and poses as a rightful user. For example, two users are communicating with each other and one of them wants to identify the other one with a password which the other party provides. In the meanwhile another user also listens to the communication and records the password. After a while the malicious user connects to the first person with the password of the second person, resultantly he is granted access. Message modification: is the alteration of a genuine message by adding, changing, deleting or reordering the message. It is a form of active attack. Active wire taping is an example of modification in which the data moving around the network is changed. The man in the middle attack is also an example of modification in which an intruder reads the messages being sent from the originator and sends modified data to the receiver with a view that both the parties will not know about the presence of the third party.

Denial of service (DOS): can occur both intentionally and unintentionally. For example an interference caused by an electron will be unintentional, or it can happen deliberately, like a malicious user sending an echo request to multiple users with the victim's address as a sender address. The request is distributed to all users and each user replies to the spoofed address of the victim. Resultantly, the attacker can disable the server with the flooding attack.

Misappropriation: is the unauthorized use of WLAN services by the attacker who tries to steal or makes other services.

Deployment of rogue WLAN devices: is a type of active attack which is mainly significant. For example, an attacker gets an access point and deploys it with a configuration that it appears as a part of the infrastructure of WLAN of that particular organization. As a result of that, a malicious user is in a position to bypass the perimeter security mechanisms installed by the organization, such as firewalls and install a backdoor into the wired network, Moreover, if any client devices unintentionally connects to the Access point installed by the malicious user, then that particular attacker is in a position to monitor as well as alter the communications between the client devices.

Monitoring of specific attacks related to WLAN is generally focused on the active attacks, mainly due to the reason that the passive attacks are strictly related to the interception of the radio transmissions and do not create any transmissions, hence the organization has got nothing to monitor electronically. However, monitoring gives due importance in case of all forms of active attacks which have been discussed. Organizations should set same perimeters for WLAN components as for any other software. Therefore, same vulnerability monitoring should be done for WLAN components by the organizations that they do for any other software, which includes identification of various patches and their application and verification of various settings of the security configuration and their adjustment as per the requirement. It is of prime importance that those actions which are performed for the wired systems of a particular organization should be performed with the same frequency for WLAN components. Apart from the general vulnerability monitoring, there is another aspect of WLAN monitoring which is termed as specific vulnerability monitoring. Vulnerabilities monitoring involves analyzing of WLAN communications and identification of the procedures and actions that are violating any policy which may include using of the wrong protocols for communications. This is not only effective in the identification of the WLAN devices that

are misconfigured, but also for those devices that are supposed to perform in a specific manner but they act in a different way than their configuration. It is particularly supportive in the scenario when the organization does not have a proper check on all the devices of that particular WLAN, which may include a laptop of any visitor and when the major concern are the WLAN devices which are not unauthorized. For example, an employee of an organization tries to attach a personal mobile device or gadget to WLAN of that organization without any proper authorization or access. It is pertinent to mention that same tools are usually utilized in this type of vulnerability monitoring that are also equally effective in attack monitoring.

Integrating the WLAN network with the suitable monitoring tool is of foremost importance. In the absence of a right set of tools which is formed on the basis of alerting, reporting of vulnerabilities or troubleshooting then in this case if a malicious user breaks into the system or for that matter violates any security policy then everything becomes reactionary and done after the event of the breach of security. With a proactive approach a person can avoid a situation in which he is questioned for a breach in the system. Wireless intrusion detection and prevention system (WIDPS) is one of the main primary tools which is widely used for the security monitoring purpose of WLAN. A WIDPS make use of different sensors. These sensors are placed at various facilities within that particular organization at selected locations. The main aim of installing these sensors is to monitor the bands of WLAN and sample traffic of various channels, which as a result allows and helps them in the identification of various attacks on WLAN and various WLAN vulnerabilities. The sensors of WIDPS are available in several forms, mainly in the form of dedicated and bundles sensors.

A dedicated sensor carries out the functions of WIDPS but it does not pass traffic on the network from source to destination. Such sensors are entirely passive, which means they only read the traffic on the network or merely sniffing the traffic on the WLAN. Some of the dedicated sensors also perform the function of analyzing the traffic, which they monitor; on the other hand, some of the dedicated sensors also forward the traffic to a dedicated server with the aim of analysis of the traffic being monitored. The dedicated sensor is normally connected to a wired network. Such sensors are planned for two types of deployments, which are namely fixed and mobile.

Fixed, in which the sensor is installed at a particular location. For installing fixed sensors an organization has also to cater for many other aspects which directly affect the working of the sensor. These aspects include the power infrastructure of the organization, access to a wired network, and other resources which helps in its management.

Mobile, in which the sensor is so designed that it is portable and it can be utilized in various scenarios, like during motion of from several locations. For example, a security administrator of a particular organization wants to find unauthorized access points so he can utilize a mobile sensor and detect illegal access points while merely walking through the buildings of that organization. In addition, many access points and various wireless switches also present some capabilities associated with WIDPS as a secondary function.

It is pertinent to mention that apart from the hardware based WIDPS, there are also software based WIDPS products that are generally host based and they can be installed on client devices of a particular WLAN. The sensor software not only identifies WLAN attacks which are in client device's range, but also the vulnerabilities of that particular client device of the WLAN, and in the end forwards this information to the management servers of the WIDPS. In addition, some sensor software's also having the capability to enforce various security policies of the WLAN. Another most important device for security monitoring of WLAN is a WLAN scanner. Such a device which is passive in nature will capture the traffic of the WLAN being transmitted within the device's antenna range. Key attributes of discovering WLAN devices are recorded by most of the passive tools. This information is very useful and can be utilized in the identification of the various vulnerabilities of the WLAN and also in the detection of the probable

unauthorized devices. Scanning tools of WLAN which are primarily used to carry out entirely passive scans do not transmit any data nor do these tools in any way affect the operation of various WLAN devices which are deployed. By the act of not transmitting any data, a passive scanning tool is in a position to remain undetected by an unauthorized or malicious user and other illegal devices. This decreases the probability of avoiding the detection by the individuals through other means which includes disconnection or disabling of unauthorized WLAN devices. In addition to the passive WLAN security tools there are also active WLAN scanning tools. The active WLAN security tools work on the information provided by the passive scans. Therefore, utilizing the information collected through passive scans, the active WLAN security tools will work in a manner that it will tend to attach to the devices of the WLAN that have been discovered and conduct various tests related to the aspects of vulnerability and penetration. While conducting active scans the organizations should be cautious and should make sure that they do not unintentionally scan devices which however are within the range of that particular organization, but are owned or used by the other organizations or individuals who do not belong to that organization. Therefore, evaluation of the physical location of the various devices is of prime importance before selecting and actively scanning them. In general, the main aim of the organization should lie on the location and identification of possible malicious devices than executing active scans. It is important to understand that the various forms of tools that have already been discussed are mere examples which are usually effective at a security monitoring of various WLANs. However, it does not mean that the types of tools other than the tools already discussed are not helpful at WLAN security monitoring. The prime importance in this case is given to the monitoring capabilities of the tools and not to the tools or for that matter the brand name of the tool.

3. Continuous Monitoring Recommendations

The organizations which use WLANs should focus on the implementation of continuous monitoring solutions for their WLANs. The continuous monitoring solutions should help the organization and should offer all of the following detection capabilities:

A. It should be able to detect unauthorized WLAN devices which also includes rogue access points and unauthorized or malicious client devices.

B. It should be able to identify the various devices of the WLAN that have not either been configured as per specifications or they are using various WLAN protocols which are weak and fragile implementation of the protocols.

C. It should also point out abnormal patterns in WLAN usage, which may include using a particular access point by an enormously high number of client devices, unusually high volumes of traffic used by a specific client device of WLAN, or a number of unsuccessful efforts in a short period of time to access a particular WLAN.

D. It should detect the use of various active WLAN scanners, for example, using war driving tools that are extensively used to generate WLAN traffic. Detection of passive sensors is not possible with the help of these monitoring controls.

E. It should identify Denial of Service (DOS) attacks. Detection of a number of Denial of service (DOS) attacks is carried out by noting the actions during time intervals and warning when a specific value is crossed. For example, a Denial of Service (DOS) attack can be indicated by a large number of events that involve the termination of the various sessions of WLAN.

F. It should also point out the man-in-the-middle attacks and impersonation. For example, a few of the WIDPS sensors can also identify when a device is trying to impersonate as another device.

All the organizations which are using WLANs should make an endeavor to have a sufficient capability of identifying the physical location of a WLAN threat which has been detected. This is usually achieved through triangulation, which uses the strength of the

signal of the threat received by each of the sensors for the estimation of the approximate distance of the threat from multiple sensors and then finding out the threat's physical location. Resultantly, enabling organization to have countermeasures for stopping the threat. For example, if a threat's location has been identified then a suitable person, which can be a staff of physical security, can be tasked to go to that respective location to address the threat.

4. Periodic Assessment

Organizations which are using WLANs should also focus on conducting periodic technical WLAN security assessments on a regular basis. To assess the WLAN security, these assessments should be performed annually. In addition to the annual assessment, it is recommended that the organizations should also give due importance to some periodic assessments at least on a quarterly basis unless all of the information about WLAN vulnerabilities and attacks, which is needed for assessment purposes is being collected through continuous monitoring of WLAN security. An organization having no widespread WIDPS coverage should make an effort for using other available tools. These tools can include use of various mobile WIDPS sensors, scanners used for WLAN and further tools that are equipped with the same capabilities of searching for rogue WLANs in the vicinities which fall outside the range of WIDPS. The organizations should give due importance to the various periodic assessments and should focus on each and every aspect of periodic assessment. The organizations should keep following factors in mind during the planning phase of the periodic assessment which are directly linked with the regularity and span of periodic assessments:

A. The location of the building or the facility which is being scanned is very important because if a building is located in the close proximity to a public area, like streets and markets or for that matter in a congested metropolitan area will have more risk of WLAN threats.

B. The security level of the data which is being transmitted on the WLAN is also very important. For example, periodic assessment of an organization which is transmitting non confidential information on its WLAN is less important than that of an organization which is using WLAN for transmission of confidential information.

C. It is also very important to know the usual traffic levels for the various devices of WLAN and how often these client devices of the WLAN are connected to and disconnected from the environment. For example, it can be distinguished as an occasional activity or fairly constant activity. This is due to the reason that during the process of WLAN scan, the discoverable devices are only the active WLAN client devices.

Table1. Comparative Analysis of Active and Passive Attacks

Passive Attack	Active attack	Comparative Analysis
Type of attack in which an unauthorized party or an attacker only monitors or listens to the WLAN communications.	An attack in which an unauthorized party or an attacker generates, alters, or disrupts WLAN communications.	In passive attacks the attacker does not generate any communication, but in active attacks the attacker generates some communication. Therefore, active attacks pose more threats.
Purpose of passive attacks is the disclosure of information or data files to an attacker without the consent of the user.	Active attacks result in the disclosure or dissemination and modification of data.	For some users disclosure of information is more important, but generally modification and alteration of data is given more weightage due to the vastness of the threat which can be a deception, disruption and usurpation.

Monitoring is not done in the case of passive attacks.	Monitoring gives due importance in case of all forms of active attacks.	Passive attacks do not generate their own transmissions, hence there is nothing to monitor electronically, but as active attacks can modify the data then monitoring of active attacks is of prime importance.

Table 2. Comparative Analysis of Monitoring Tools

Dedicated	Bundled	Comparative Analysis
A dedicated sensor performs WIDPS by only sniffing the network traffic.	Many APs and wireless switches offer some WIDPS capabilities as a secondary function.	It primarily depends on the organization to select between various types of monitoring tools according to the nature of the threats. However, due to the ever increasing nature of threats one must go for dedicated monitoring tools.
Dedicated monitoring tools can either be fixed or mobile.	Bundled monitoring tools are always fixed.	Dedicated monitoring tools can be used from multiple locations or while in motion while bundled monitoring are fixed. The aspect of mobility clearly depicts the superiority of fixed over bundled monitoring tools.

5. Conclusion

The challenges faced by the organizations using Wireless Local Area Networks (WLANs) are manifold. Due to the very nature of wireless networks, at times even the most confident network administrators find it difficult to manage and secure the wireless network. With ever increasing threats to Wireless Local Area Networks the organizations and users of WLAN should always be proactive when it comes to WLAN security. The organizations and personnel related to security must deeply analyze the nature of threats which are being posed to an organization or an entity and should select the right set of monitoring tools to counter them. The organizations should also make an endeavor to implement continuous monitoring solutions for their WLANs, which will ultimately help the organization to strengthen the security infrastructure.

References

[1] Q. Li, N. Memon and H. T. Sencar, "Security issues in watermarking applications - a deeper look", Proceedings of MCPS, ACM, New York, **(2007)**, pp. 23-28.
[2] H. Nyeem, W. Boles and C. Boyd, "Developing a digital image watermarking model", Proceedings of DICTA, IEEE, Piscataway, **(2011)**, pp. 468-473.
[3] H. Nyeem, W. Boles and C. Boyd, "Counterfeiting attacks on block-wise dependent, fragile watermarking schemes", Proceedings of the 6th International Conference on Security of Information and Networks, **(2013)**, pp. 86-93.
[4] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding -a survey", Proceeding of IEEE, vol. 87, **(1999)**, pp. 1062-1078.
[5] Z. Jian and E. Koch, "A generic digital watermarking model", Comput. Graph, vol. 22, no. 4, **(1998)**, pp. 397-403.
[6] T. Mittelholzer, "An information-theoretic approach to steganography and watermarking", Proceedings of Information Hiding, Springer, Heidelberg, vol. 1768, **(2000)**, pp. 1-16.
[7] A. Adelsbach, S Katzenbeisser and A-R Sadeghi, "A computational model of watermark robustness", Proceedings of Information Hiding. LNCS, vol. 4437, **(2007)**, pp. 145-160.
[8] J. A. O'Sullivan, P. Moulin and J. M. Ettinger, "Information theoretic analysis of steganography", Proceedings of the International Symposium on Information Theory, IEEE, Piscataway, **(1998)**.
[9] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game", IEEE Trans. Inform. Theor., vol. 48, vol. 6, **(2002)**, pp. 1639-1667.
[10] C. Cachin, "An information-theoretic model for steganography", Inform. Comput., vol. 192, no. 1, **(2004)**, pp. 41-56.

[11] I. J. Cox, M. L. Miller and A. L. McKellips, "Watermarking as communications with side information", Proceedings of IEEE, vol. 87, **(1999)**, pp. 1127-1141.
[12] A. Adelsbach, S. Katzenbeisser and H. Veith, "Watermarking schemes provably secure against copy and ambiguity attacks", Proceedings of Workshop on Digital Rights Management, ACM, New York, **(2003)**, pp. 111-119.
[13] M. Barni, F. Bartolini and T. Furon, "A general framework for robust watermarking security", Signal Process, vol. 83, no. 10, **(2003)**, pp. 2069-2084.
[14] P. Moulin, M. K. Mihcak and G.-I. Lin, "An information-theoretic model for image watermarking and data hiding", Proceedings of ICIP, IEEE, Piscataway, vol. 3, **(2000)**, pp. 667-670.
[15] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding", IEEE Trans. Inform. Thor., vol. 49, no. 3, pp. 563-593.
[16] M. Holliman and N. Memon, "Counterfeiting attacks on, oblivious block-wise independent invisible watermarking schemes", IEEE Trans. Image Process, vol. 9, **(2000)**, pp. 432-441.
[17] H. Nyeem, W. Boles and C Boyd, "Utilizing least significant bit-planes of RONI pixels for medical image watermarking", Proceedings of DICTA, IEEE, Piscataway, **(2013)**, pp. 1-8.
[18] A. Khan and A. Sarfaraz, "Vetting the Security of Mobile Applications", Science International, vol. 29, no. 2, **(2017)**, pp. 361-365.
[19] A. Khan, M. Sohaib and F. M Amjad, "High-Capacity Multilayer Framework for Highly Robust Textual Steganography", Science International, vol. 28, no. 5, **(2016)**, pp. 4451-4457.
[20] A. Khan, U. Tariq, J. Shabbir and S. Hassan, "Cloud Security Analysis for Health Care Systems", International Journal of Computer and Communication System Engineering, vol. 3, no. 1, **(2016)**, pp. 1-8.
[21] S. Azeem, A. Khan, E. Qamar, U. Tariq and J. Shabbir, "A Survey: Different Lossless Compression Techniques", International Journal of Technology & Research, vol. 4, no. 1, **(2016)**, pp. 1-4.
[22] M. Shah and A. Khan, "Implementing User Authentication Service for Cloud Network", Science International, vol. 28, no. 6, **(2015)**, pp. 5301-5306.
[23] A. Khan, "Comparative Analysis of Watermarking Techniques", Science International, vol. 27, no. 6, **(2015)**, pp. 6091-6096.
[24] A. Khan, "Robust Textual Steganography", Journal of Science, vol. 4, no. 4, **(2015)**, pp. 426-434.
[25] U. Khadim, A. Khan, B. Ahmad and A. Khan, "Information Hiding in Text to Improve Performance for Word Document", International Journal of Technology and Research, vol. 3, no. 3, **(2015)**, pp. 50-55.

Authors

Ahmed Khan, is a lecturer in computer science faculty of COMSATS Islamabad. His PhD is in Information Security from NUST Military College of Signals Pakistan. Furthermore, Iqra University has awarded MS-CS degree in 2015 and well experienced in developing various projects using Java Desktop, Web and Android Applications using advance frameworks in different software companies and institutes/ universities since a 2012-Till Date. In 2012, he got BS-CS degree from The Islamia University of Bahawalpur with specialization in software engineering. He is a critical reviewer of ISI indexed Journals. He has 22 research publications in many well reputed journals with an interest in image watermarking software development, information security and computer forensics.

Aliyah Sarfaraz, is lecturer in computer science faculty of COMSATS Islamabad and PhD student in Department of Computer Science at UNSW Australia. In 2015 she got her MS from University of Seoul, South Korea in Computer Graphics. In 2012, she got BE-CS degree from The Balochistan University of Engineering & Technology with Gold Medal. Her research interests include multi-variate splines on root lattices, volume rendering and GPU computing.

