Encryption as an Impressive Instrumentation in Decrease Wireless WAN Vulnerabilities

Seyed Hasan Mortazavi Zarch, Farhad Jalilzadeh, Madihesadat Yazdanivaghef

Abstract- The security of wireless WANs(world area network) has been a source of concern for businesses and individuals who are aware of its advantages due to its flexibility. With the increase in the use of wireless WANs for enterprises and homes, where information assets are shared continually, security is of the essence. With the increase in e-commerce and e-services, there is the risk of identity and credit card theft. Encryption is seen as a major tool in the line of defense of wireless WANs. This article discusses the various security protocols used in wireless WANs and how effective they are in keeping wireless WANs secure. The risks of using these protocols are outlined and recommendations for securing wireless WANs are reviewed.

Index Terms- wireless WAN security, Encryption, WEP, WPA, 802.11 protocols.

I. Introduction

Wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location. With the benefits of Wi-Fi there are also some risks which users should be aware of. Without any security implemented, unauthorized users may steal data or load malicious code onto the network with the intention of creating havoc. Unlike wired networks, the radio signal produced by wireless networks can penetrate walls, ceilings, floors and are therefore not confined to a building. Hackers can effortlessly pick up these signals from the outside of the building using easily available wireless detection tools. Medium to large scale businesses transmit sensitive data. These include personal data of clients, company data which should not be exposed to competitors, amongst others. Whilst a typical user would normally not transmit sensitive data, the increasing growth of the use of e-commerce and e-government services has meant that more sensitive data is being transmitted by citizens to local and federal government. It can be obviously seen that the interception of such data may be of serious harm to citizens. Indeed, the US government has used queries such as "What was the figure on your last tax return?" to *authenticate* a caller. The reason this was chosen as an authentication question was because it was felt that *only the legitimate citizen* would have the answer [1].

Many WWANs used in the home still operate with no measure of encryption, and this is certainly inappropriate when using electronic services. However, there does arise something of a problem for the home user when establishing a WWAN, namely which encryption protocol to use. This paper considers the major encryption protocols, their strengths and weaknesses and offers recommendations in securing WWANs. The majority of wireless networks use the IEEE 802.11 standard for communication. Initially the IEEE 802.11b was the de-facto security standard for wireless networking technology for small businesses and home users, with all Wireless Access Points equipped with Wired Equivalency Protocol (WEP).

Flaws in WEP were soon discovered and in response to this, the 802.11i task group was developed to address the major problems with security. They addressed three main security areas: authentication, key management and data transfer privacy. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) as a Wi-Fi standard, which accelerated the introduction of stronger security. As the security standards have evolved, other wireless security options have become available which are preinstalled on devices. These include WPA and Temporal Key Integrity Protocol (TKIP).

However, with WPA, enterprise managers discovered that the WWAN was secure but not truly mobile and reflective of user demands. [2] Due to user roaming and the resulting changes in static IP addresses, WPA required re-authentication, which posed problems with current 2G WWAN implementations. In addition, poorly chosen, short, human-readable pass phrases used in WPA can be cracked with a robust dictionary attack offline and without access to the network [3].

Initially, when Wi-Fi networking was in its infancy, war-walking, war-driving and war-chalking were well publicized phenomena. Developed by Peter Shipley in April 2001, these terms describe the process used by hackers walking or driving around areas looking for unsecured wireless networks. Symbols were left on the walls or pavements to indicate the security status of nearby Wi-Fi points. War-driving did highlight the worrying results that firstly, a large proportion of Wi-Fi users do not enable any form of encryption and secondly, that the standard wireless encryption protocol (Wired Equivalency Protocol WEP) can easily be cracked.

Even after much publicity about wireless encryption and new improved protocols were made available, a survey on wireless security in San Francisco revealed out of 2287 access points and 421 client cards, 35% of all business networks were found to be unsecured and 28% of all access points were found to be displaying default values. [4].

II. Security Protocols and Encryption

2.1 WEP

In 1997, WEP (Wired Equivalent Privacy**)** was developed by the 802.11b task force with the introduction of wireless technology, and was the first encryption protocol to be deployed with wireless networks. WEP incorporates two types of protection, a secret key and encryption.

WEP stands for Wired Equivalent Privacy and protects wireless communication from eavesdroppers. WEP also prevents unauthorized access to wireless networks. The WEP algorithm works on the basis of a secret key shared between a mobile device (e.g. PDA, cell phone, tablet PC) and an access point [5]. Packets are encrypted using the key before transmission. An integrity check ensures that packets are not changed during the transmission. Although WEP does not purport to state how the key is shared between sender and receiver, most systems share a single key among all mobile devices and wireless access points. More sophisticated key management techniques can be used to help defend from the attacks we describe.

WEP uses the RC4 encryption algorithm, known as a stream cipher, which expands a short key into an infinitely long random character stream. Plain text is XOR'ed by the sender to generate cipher text, which is then transmitted. Although the cipher text can be obtained in transit, hackers usually cannot understand the content of the message because they do not have access to the key that was used by the sender for encryption. A trusted receiver, on the other hand, can decipher the contents of the message because it has a copy of the same key that was used by the sender to encrypt the message. However, if hackers modify the encrypted stream of data in transit, the receiver will receive incorrect data. If 2 such encrypted messages are intercepted by hackers, then XOR of the cipher text yields the XOR of the original messages. This knowledge can aid a determined and skillful hacker to mount statistical attacks to obtain the original plain text message.

Due to these vulnerabilities, the encryption algorithm used by WEP is not the strongest to protect against all attacks.

2.1.1 Problems with WEP

WEP has several serious inherent problems. It does not meet its fundamental security goals of wired-equivalent confidentiality. It also fails to meet the expected goals for integrity and authentication.

WEP has two generic limitations. First, the use of WEP is optional, and as a result, many real installations never even turn on encryption. Second, by default, WEP uses a single shared key common to all users of a WWAN, and this common key is often stored in software-accessible storage on each device [6]. If any device is lost, stolen or compromised, the only solution is to change the secret key in all of the remaining devices. Since WEP does not include a key management control, distributing the new secret key to all the users is a tasking process.

In practice, the most serious problem with WEP is that its encryption keys can be recovered through crypt-analysis. It was discovered that a passive attack could recover the RC4 key after eavesdropping on the network for a few hours and collecting 100,000-1,000,000 packets. [7] A hacker could use an XOR function to mathematically link two packets of a session that have been processed with the same IVs, i.e. identical RC4 keys, which can be used to recover the key. Another fault with the WEP protocol was that the authentication only verifies the client machine, not the actual user accessing the machine. This occurs as the only key condition is that the WWAN card and the access point use the same algorithm. Therefore, everyone on the local network uses the same secret key, which the RC4 algorithm uses to generate an infinite, pseudorandom key stream. Both the 40-bit and the 104-bit keys are vulnerable to attacks, due to various weaknesses internal and external to the protocol supporting WEP.

These vulnerabilities include the heavy reuse of keys, the ease of data access in a wireless network, and the lack of any key management within the protocol. For example, the IV will be duplicated within 5 hours at a busy access point when 1500-byte packets (the standard Maximum Transition Unit for an Ethernet network) are transmitted at a rate of 11 Mbps. It is therefore possible to determine the RC4 key stream over several hours after the IV has been repeated.

Originally, it was thought that increasing the key size from 40-bits to 104-bits would overcome some of the security problems; however the implication of 128-bit WEP has caused problems for heterogeneous environments in which interoperability was an issue. In 2005, using a combination of statistical techniques focusing on unique IVs captured and brute-force dictionary attacks to break 128-bit WEP keys, the U.S. Federal Bureau of Investigation cracked WEP in 3 minutes [8]. With the proper equipment, it is possible to

Eavesdrop on a WEP-protected network from distances of a mile or more away from the target [6]. With the tools and information available on the Internet, an inexperienced hacker could crack WEP encoded data in a matter of days.

2.2. TKIP

Temporal Key Integrity Protocol (TKIP) was the immediate replacement for WEP, which aimed to fix the problems, associated with WEP including small initialization vectors (IV) and short encryption keys. TKIP is a suite of algorithms that wrap around the WEP protocol to make it more secure. The reason why TKIP is an improvement on WEP is that it rotates the temporal keys; therefore, a different key is used for each packet. Each packet transmitted using TKIP has a unique 48-bit serial number that is incremented every time a new packet is transmitted. Each time a wireless station associates with an access point, a new base key is created.

The base key is built by hashing together a special session secret with some random numbers generated by the access point and the station as well as the MAC address of the access point and the station. This mixing operation is designed to put a minimum demand on the stations and access points, yet have enough cryptographic strength so that it cannot easily be broken. Putting a sequence number into the key ensures that the key is different for every packet.

This resolves another problem of WEP, called "collision attacks," which can occur when two messages have the same key. This could potentially be a problem if one message says “I agree to pay X $500.00 on 01/01/2007” and the second message says “I agree to pay X $500,000.00 on 30/12/2010”. The attacker could get the victim to digitally sign the first message, but claim the signature was for the second message of a greater value and use the key as proof of authentication [9]. With different keys, collisions are prevented.

TKIP also utilizes an integrity-checking feature called Message Integrity Check (MIC or Michael). This part of TKIP closes a hole that would allow a hacker to inject data into a packet, which allows the hacker to deduce the streaming key used to encrypt the data. MIC uses a cryptographically protected one way hash in the payload, which ensures packet tampering detection occurs immediately upon decryption. Compared to WEP, TKIP is a costly process and may degrade performance at many access points, where it can consume every spare CPU cycle.

TKIP also uses RC4 as the encryption algorithm, but it removes the weak key problem and forces a new key to be generated every 10,000 packets. In addition, it hashes the initialization vector (IV) values that were sent as plaintext in WEP. TKIP is useful as it can be used on old hardware, which supports WEP but not WPA, and new hardware that only supports WPA.

2.3. WPA

WPA (Wi-Fi Protected Access**)** was created by the Wi-Fi Alliance once the flaws associated with WEP were discovered, and used as an intermediate standard until the IEEE 802.11 working group developed a more secure protocol. WPA was based on the WEP protocol, but utilizes the stronger encryption technology used in TKIP, which offers pre-packet key mixing and a message integrity check. Applicable to home as well as enterprise users, the standard is designed to run on existing hardware as a software upgrade and is forward-compatible with the new IEEE 802.11i standard.

To improve message protection, WPA utilizes the Temporal Key Integrity Protocol, which is designed to address all known attacks against, and deficiencies in, the WEP algorithm. TKIP defends against replay and weak key attacks, detects message modification, and avoids key reuse. To improve user authentication and access control, WPA implements the Extensible Authentication Protocol (EAP) and the IEEE 802.1x standard for port-based access control. This framework uses Radius (Remote Authentication Dial-in User Service), a central authentication server, to authenticate each user on the network. Rather than being an authentication protocol,

EAP is a transport protocol tailored to the needs of upper-layer authentication protocols. It provides a plug-in architecture for numerous popular ULA protocols in use today [10]. These protocols facilitate a mutual authentication exchange between a mobile station and the Radius server residing on the network. They also generate keys for use on the wireless link between the mobile station and access point. In a home or small office/home office (SOHO) environment, where there is no central Radius server or EAP framework, WPA runs in a special home mode, called *preshared key*, for which a user must enter a password before a mobile station can join the network. ULA is not supported in preshared key mode.

Although WPA is stronger than WEP, it is, however, vulnerable to Denial-of-Service attacks. The goal of a DoS attack is to deny legitimate users access to a resource by disrupting or attacking the resource itself. For example, an attacker could generate numerous connection requests to a server, effectively blocking access to this server for many hours. DoS attacks carried out at layer 2—the media access control (MAC) layer of Wi-Fi networks exploit a management frame's lack of encryption and integrity protection even when WPA or 802.11i is utilized. An attacker can easily forge management packets and send disassociation or DE authentication packets to the mobile station or access point, thereby denying or delaying legitimate packets. Radio-frequency-based DoS attacks at a Wi-Fi network's physical layer are also possible. There are no efficient countermeasures against DoS attacks [10].

Also, there is the issue of key-scheduling. WPA obtains the 128-bit *temporal key* from the EAP framework during authentication and inputs it into a key hash function together with the 48-bit *transmitter address* and a 48-bit *initialization vector*. The hash function outputs a 128-bit WEP key, or packet key. This key is used for only one WEP frame since the initialization vector is implemented as a counter that increases with each new package. Because each package contains the initialization vector in clear text, an attacker can obtain all utilized initialization vectors [11]. For example, let IV32 denote the most significant 32 bits of the 48-bit initialization vector. Given two WEP keys based on the same IV32, an attacker can use software to determine the temporal key. It typically takes about 30 hours to run such a program on a 2.53-GHz Intel Pentium 4, but the processing time is only six or seven minutes when four or more WEP keys based on the same IV32 are available. WPA security relies wholly on the secrecy of all WEP (packet) keys. The attacker can determine the WEP keys based on the temporal key and decrypt all packets generated during the complete session.

The attack does not imply that WPA is broken, but it underlines the importance of keeping every WEP key secret. In a well-designed system, cracking two packet keys should not enable an attacker to determine the session key. Thus, it can be said that WPA has a serious design weakness.

The Transport Layer Security protocol is the default ULA method for WPA. TLS (also denoted as EAP-TLS) is based on the Secure Socket Layer 3.0 protocol specification. SSL is a public-key, cryptography-based confidentiality mechanism. While the Wi-Fi Alliance has recommended that all WPA products should support TLS, manufacturers can choose another ULA method. Although TLS will likely be the most popular method, using different ULA protocols creates interoperability problems between different systems. If most enterprise WPA systems use TLS; it could become the most popular ULA protocol in systems implementing the new 802.11i security standard.

2.4. Wi-Fi Protected Access 2 (WPA2)

The current standard for wireless security is 802.11i or WPA2. In June 2004, the IEEE formalized 802.11i, shortly after the Wi-Fi Alliance released WPA2. While the two are not strictly identical, from a practical standpoint the two terms are used interchangeably. If you buy a wireless access point or router with either term on it, it provides the same level of security. The WPA2 designation means that the equipment is interoperable with other equipment bearing that designation. WPA2 and 802.11i incorporate the security enhancements that were part of WPA [12].

The IEEE 802.11i standard WPA2, addresses three main security areas: authentication, key management, and data transfer privacy. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is backward compatible with WPA. Like WPA, WPA2 is also available in Personal and Enterprise modes. WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. However, although WPA2 implements the full standard, it will not work with some older network cards.

The encryption algorithm used in the 802.11i security protocol is AES-Counter Mode CBC-MAC Protocol (AES-CCMP). It uses the AES block cipher (see below), but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBCMAC). The counter mode uses an arbitrary number that changes with each block of text, making it difficult for an eavesdropper to spot a pattern. The CBC-MAC protocol (Cipher Block Chaining-Message Authentication Code) is a message integrity method, which ensures that none of the plaintext bits that were used in the encryption were changed.

AES so far has proved unbreakable, and meets the U.S. government's Federal Information Processing Standard (FTPS) for security, FIPS 140-2. Other advancements in WPA2/802.11i include its message authentication code and its four step handshake, used to establish a second key between the client and AP. These and other features guard against unauthorized access to WPA2/802.11i networks.

802.11i also speeds roaming from one access point to the next. Previously, the station needed to perform a complete 802.1X authentication each time it associated with a new access point. With 802.11i, when the station returns to an access point it already authenticated with, it can reuse the PMK established with that access point to omit 802.1X authentication and perform only the four-way handshake. This speeds transitions between access points. Additionally, the station may "pre-authenticate" to a new access point it intends to roam to while still associated with the current access point; this allows the station to only perform a four-way handshake once it does roam [13].

2.5. Extensible Authentication Protocol

WPA and WPA2 enterprise modes both utilize the Extensible Authentication Protocol (EAP) as an authentication framework. EAP is an 802.1X standard that allows developers to pass security authentication data between the RADIUS server, the access point and wireless client. EAP has a number of variants, including EAP MD5, EAP-Tunneled TLS (EAP-TTLS), Lightweight EAP (LEAP), and Protected EAP (PEAP). EAP resides in the access point and keeps the network port disconnected until authentication is completed. Depending on the results, either the port is made available to the user, or the user is denied access to the network [1].

2.6. Robust Secure Network (RSN)

Robust Secure Network (RSN) is a protocol used for establishing secure communications over an 802.11 wireless network, and is an element of the 802.11i standard. RSN dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless access point and wireless clients. This means that as new threats are discovered, new algorithms can be added. Transitional Security Network (TSN) is a specification that is designed to allow RSN and WEP to coexist on the same wireless WAN [1].

III. Recommendation

In order to secure a wireless network users should follow a number of procedures to prevent the network from being penetrated. From the outset, some devices have the security settings disabled as the default option. Therefore it is important to switch on the security settings when setting up the device. Wireless detection tools can determine the level of security and an unsecured network is an easy target even for novice hackers.

Although WPA and WPA2 are securer encryption protocols than WEP, if the access point only supports WEP it is worthwhile enabling it. This will prevent neighboring Wi-Fi users without the knowledge or intention to hack from sharing bandwidth. If someone has the ability and intention to hack then WEP is not very protective. However, to make it more secure the user should make the password difficult to guess. Using a selection of random letters and numbers that are not in the dictionary could prevent attacks by programs that carry out dictionary attacks. It is also important to change the password regularly, as an attack may occur over a long period of time if the intruder is determined to gain the information.

It is important to weigh up the costs of how sensitive the data is before deciding whether to use it or not. For the home or small office, the payoff for breaking into a wireless network is considered by some simply too small for an attacker to expend the effort required [14].

When using WPA or WPA2 encryption in consumer mode, the password should contain a minimum of 20 randomly selected letters. The manufacturers default SSID, usernames and passwords are well known to hackers. Therefore, it is likely that if the user has not changed the SSID, then the username and password has also not been changed. This would enable the hacker to change the configuration of the access point to allow easy access. When changing the SSID, it is important not to use personal details that could identify the owner. For example, the house number and street name, or business name. This would inform the hacker with the exact location of the network. Using a complicated SSID will avoid identifying the access point but may raise suspicion from hackers who may think the user has something to hide.

Furthermore, the software supplied with access points can be too complicated for the average user and the security options are often difficult to find within the software or located under the heading “Advanced Settings” which may prevent some users from utilizing it [18]. Therefore, it is recommended that software designers ensured that security settings are readily accessible to users and that help information should be made intelligible for both technical and non-technical users.

In addition to offering specific guidelines for what to do and improving the user’s access to how to do it at the machine, there are other ways of encouraging improvements in wireless security through awareness raising and direct assistance.

For connection to Wi-Fi hotspots, connecting to a company’s network through virtual private networks (VPNs) or Secure Sockets Layers (SSLs) could provide some level of security. A VPN can also be a good security solution for a large company, especially since its IT department can reinstall VPN clients on the employees’ laptops. The VPN secures the network connections from the laptops all the way to the VPN server on the company network.

It is more difficult to implement a VPN in a university or other environment where users must install their own VPN clients. Users are likely to employ multiple operating systems and OS configurations, requiring numerous VPN clients. Even if it were possible to find clients that are stable on all platforms, many users would have trouble installing and configuring them.

Wi-Fi users can use SSL and the Secure Shell protocols in a hotspot employing a captive portal with no encryption of user data. HTTPS uses SSL to enable secure access to Web pages. Some mail protocols, such as version 3 of the Post Office Protocol and the Internet Message Access Protocol, also employ SSL.

IT in businesses should be able to easily configure, distribute, monitor and maintain network Policies enterprise wide, as well as define which resources users and groups can access and control their roaming privileges. A wireless WAN system should allow for policies to be assigned by domain or for the entire network. For maximum flexibility, IT should be able to manage polices from anywhere in the organization. The ability to provision guest access and deliver basic network services to visitors is essential. For maximum protection, Guest traffic should be kept secure and separate from internal traffic. The ability to provision multiple virtual services is particularly useful in multi-tenant situations, so different companies can safely share the same wireless infrastructure, while IT is assured that each company's traffic stays isolated and private [15].

IV. Conclusion

As wireless world area networks become integral parts of enterprise-level networks, it has become imperative that the wireless components of the network be as secure as the wired network.

Although the early versions of WWANs were not designed for security, standards and methods are emerging for securing 2G broadband, enterprise-capable WWANs. With 802.1X and 802.11i protocols, there are now good choices for encryption and authentication. These emerging security features must be implemented in order to assure the security of information on the wireless networks. With careful planning and due diligence, a wireless network can be as secure as a wired network. Human factors are as important as technical factors in ensuring wireless security.

As the increase of e-commerce and e-services to both home and business users gathers momentum, the risk to these users of suffering loss of control of information – interception, insertion, deletion, corruption – and related physical assets will become of increasing concern both to individuals and to society in general. There is the need to incorporate wireless security into the curricula of information security programs to maintain the relevancy of students' knowledge in today's world.

There is no doubt that encryption is an important tool in any computer security tool kit, its importance should not be overrated. Encryption does not solve all computer security problems, and other tools must complement its use. Furthermore, if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system [17]. Weak encryption can be worse than no encryption at all because it gives a false sense of security.

References

[1] C. Maple, H. Jacobs, and M. Reeve. Choosing the right wireless LAN security protocol for the home and business user. In Proceedings, First International Conference on Availability, Reliability and Security. September, 2007.

[2] Bhagyavati, W.C. Summers and A. DeJoie. Wireless security techniques: an overview. InfoSecCD Conference. September, 2004.

[3] R. Moskowitz. Weakness in pass phrase choice. Wi-Fi Networking News, Sourced: October 15, 2006. http://wifinetnews.com/archives/002452.html, November 4, 2007

[4] RSA Security. The wireless security survey of San Francisco. RSA Security Inc. http://www.securitymanagement.com/library/rsa_wirel ess0606.pdf

[5] K. Curran and E. Smyth. Demonstrating the wired equivalent privacy (WEP) weaknesses inherent in Wi Fi networks. Information Systems Security 15(4), pp. 17-38. September, 2006.

[6] N. Cam-Winget, R. Housley, D. Wagner and J. Walker. Security flaws in 802.11 data link protocols. Communications of the ACM, 44(5):35-39, May, 2004.

[7] S. Fluhrer, I. Mantin, and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, Selected Areas in Cryptography 2005 vol. 2259 of Lecture Notes in Computer Science, Springer, 2001, pp. 1-24.

[8] H. Cheung, "The Feds can own your WAN too", 2005. Sourced: 7 December 2006 http://www.tomsnetworking.com/Sectionsarticle111-page1.php

[9] "Hash Collision Q&A", Cryptography esearch, 2005 updated February 16, 2005. Sourced: 9 November, 2007. http://www.cryptography.com/cnews/hash.html

[10] K.J. Hole, E. Dyrnes, and P. Thorsheim. Securing Wi-Fi networks. Computer Pages 28-34. July, 2008.

[11] V. Moen, H. Raddum, and K.J. Hole, "Weaknesses in the Temporal Key Hash of WPA," ACM Sig-Mobile Mobile Computing and Comm. Rev., vol. 8, no. 2, 2009 pp. 76-83.

[12] D. Robb. 802.11i brings more security to WWANs. Business Communication Review. Pages 52-54, April, 2006.

[13] P. Funk. 802.11i secures the WAN. Communication week. September, 2005. Sourced: 20 November, 2007. http://www.comnews.com

[14] N.R. Mead, and G. McGraw. Wireless security's future. IEEE Security and Privacy, pages 68-72, July 2008. IEEE Computer Society Press.

[15] D. Simone. (2006, 02//). Make WWAN more secure. Commun. News 43(2), pp. 36-38.

[16] A. Bittau, M. Handley and J. Lackey. The final nail in WEP's coffin. Proceedings of the 2006 IEEE Symposium on Security and Privacy. 2006. IEEE Computer Society Press.

[17] C. P. Pfleeger, and S. L. Pfleeger. Security in Computing. Prentice Hall, Upper Saddle River, New Jersey, 2003

[18] S. Furnell, Why users cannot use security. Computers & Security., pp. 274-279. 24, 2005.

Authors

First Author – Seyed Hasan Mortazavi zarch, Email: hassanmortazaviy@yahoo.com
Second Author – Farhad Jalilzadeh, Email: farhad.jalilzadeh2006@gmail.com
Third Author – Madihesadat Yazdanivaghef, Email: madi.yazdani@gmail.com