Marcin Kołodziejczyk*

# Applying of Security Mechanisms to Low Layers of OSI/ISO Network Model

## 1. Introduction

The purpose of this article is to describe some security levels and restrictions which may be used in low layers of network. Before we start, we should realize that people started to care about network security much more later than networks were involved. At the begin, there was no security, there were another needs and issues like too slow connections, too many faults on physical links, etc. Internet was not so popular and only small group of people had access to the network. So, there was no reason to design secure protocols. The simplest protocol was the best. For example Ethernet is much more popular than Token Ring and nobody cares that Token Ring guarantee that the network frame will be sent after some, specific time and Ethernet does not do that. Many protocols, which are used today, were designed many years ago. There was no reason to think about intruders. Today, networks' attacks are a big problem, that there are no security mechanisms in many popular protocols. For example, there is no certainty that MAC address is correct, not exchanged. Almost every network device allows changing this address. ARP protocol asks who has this address and everybody can answer: „this is my address". There are many other examples. I will try to describe some of them and try to answer for the question: „is there any way to make network connections more secure?".

## 2. Physical security

Before we start to discuss about possible network attacks, we should discuss about physical security of networks. I have seen many networks which were susceptible to physical attack. Such attack can be invisible because of such mechanisms like broadcast or copying a file. Many attacks can be also ignored, because symptoms of attack may be very small like short term damage of network. Many devices can be stolen, many data can be copied to

* Wydział Elektrotechniki, Automatyki, Informatyki i Elektroniki, Akademia Górniczo-Hutnicza w Krakowie

external drive and many times it is much easier than typical network attack. How many people are conscious that they have shared disks in public, wireless network and they granted access to everybody with no password? What would happen if such, shared data were a secret and important data for the company? Who cares that computers may be attacked during network surfing in public hot spots? Wireless signal can be also used to attack and it is very important to be aware of it.

## 3. Sniffing and spoofing

One of the most popular network attacks is a sniffing. The idea of Ethernet is to send network frames to every connected device in the "ether". The destination device should check destination address and accept or ignore received frame. In this situation, there is no problem with sniffing all data sent over the network. The performance requirements were the reason of using bridges or switches[1)]. These devices divide the network to some areas, named collision domains. Every switch and bridge checks source addresses in network frames and bind them with his physical interface. It protects the network against simple sniffing attacks. There is no simple way to listen the data, the attacker is interested in. The data are sent only to specific device, not to all devices. The idea of the Ethernet is well described in [3]. However, there is no authentication in 2nd network layer, so every device can say: "my address is X", where X means fictitious physical address. However sniffing may also be used for diagnosing purpose and is needed in many situations. It shows the basic conflict. We want to have some simple diagnostic tools. On the other hand, there is a necessity to make the network secure.

Another simple method is called spoofing. There is no authentication and as I mentioned in previous paragraph, every device can laying and exchange source addresses in sent frames, for example it is possible to send correct "ARP response" frame with wrong MAC address. This vulnerability is well known and used with ARP poisoning techniques (Fig. 1). There are no states in ARP protocol, so it is hard to connect specific request with specific response. If a host does not know MAC address of destination device, ARP request "who has such address" is sent to every other host in the local network. Only one host should reply for this request. ARP responses are cached for a while, for example few minutes. If a source host has specific record in ARP cache there is no reason to send a request "who has such address?", because destination address is known. However, intruder may send ARP replies to the victim, without the "ARP requests". It causes the change in a victim host. ARP cache is not correct, is poisoned. Since now, a victim will sent all packets to the intruder instead of correct destination device. Both methods, sniffing and spoofing are well described in many publications, including [1].

---

[1)] Network bridge has only 2 interfaces (ports), but switch have more.

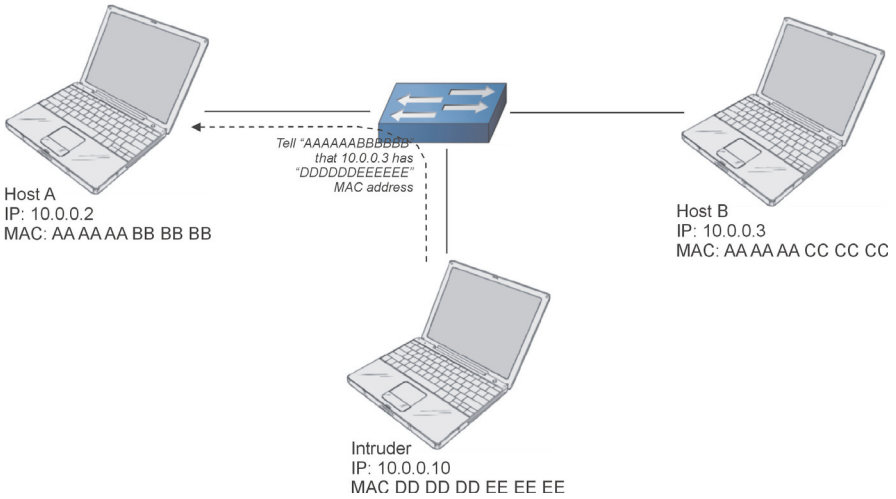


**Fig. 1.** ARP poisoning

Spoofing can be also used against Dynamic Host Configuration Protocol (DHCP). The typical scenario is that a new host in the network asks DHCP server about IP address which can be used. DHCP server reserves one of free addresses for asking host for specific time period and then sends the answer to specific MAC address. As it was described, MAC address can changed, so the intruder may send many DHCP request with many different MAC addresses. This is a simple method for reservation all IP addresses in DHCP server. This may cause the situation, that no one else can reserve a new address and connect to the network.

There is a question what security mechanisms may be used? What can make 2nd network layer more secure? First of all, network should be divided into collision domains by switches. It protects the network against the basic sniffing. We can create static ARP records on every host and block ARP packets at all. This solution is very complicated in big companies with many network devices. It is hard to maintain correct entries in all ARP tables on every host. The resolution may be IPv6 protocol. ARP protocol may be not used in some implementations of IPv6 because of huge address space and auto-configuration mechanism. The author is considering if ARP broadcasting can be used on every switch. However, author has not seen the switch with such functionality. If ARP responses were sent to every host in the network, ARP spoofing attack could be discovered in very easy way. It is known that IP protocol requires checking if there is no IP conflict in the network. Perhaps, similar mechanism in 2nd layer would increase the security level of Ethernet.

## 4. Ipv4 vs. IPv6

IP protocol (Internet Protocol) is a stateless protocol. This fact allows to some abuses in 3rd – network layer in OSI/ISO model. There are no doubts that IP version 4 is one of the most

popular protocol all over the internet. The IP header contains few interesting fields like source and destination addresses, time to live, identification, flags and fragment offset. Routers have to forward IP frames as soon as possible – this is a performance requirement. The second problem is that the route of 2 packets with identical addresses can be different. Third, important thing is that IPv4 packets can be divided to few smaller packets by routers. These three things can cause some problems in the third layer. Many network devices can crash because of strange fragment offset's value in IP packets. What would happen if begin of second part of packet (counted from offset value) was before the end of first packet? Another problem is what will happen if too many uncompleted packets with different identification number are received? Destination device would receive huge number of unfinished packets with a whole in the middle of every malicious packet. I doubt that all network devices and software are tested against such tricks. I think many of them are vulnerable. The next thing is that TTL field can be used for checking operating system. Different systems put different values to this field. This field can be also used to determine number of routers between sender and current host or router. TTL is decremented usually by 1 on every router and initial value is usually 32, 64 or 128. Moreover, if we do not want somebody to have a router, we can decrement TTL to 1. In this case, additional router (unwanted by us) decrements this value to 0 and packet will die, will be not forwarded. IPv4 can contain additional options. One of them is very interesting from security point of view. A "Security" option may be used by military routers to determine more or less secure routes, for example according to rule that confidential data should not be sent through hostile countries.

IP version 6 is a successor of IPv4. It is a little strange, because this protocol is more than 10 years old and IPv4 is still more popular than new version IPv6. However, the number of free IPv4 addresses is not so big and becomes smaller every day, so Ipv6 will be implemented in many systems and used in the nearest future. The header in new version of IP protocol is much simpler. Moreover routers can't divide packets to smaller parts any more. These facts efficiently prevent from few performance attacks possible against IPv4. The author is wondering about "flow label" usage. Perhaps this field can be used for DoS[2)] attacks.

## 5. IPSec protocol

Basic, typical TCP/IP networks are almost not secured. There are no doubts that encryption and integrity control should be provided in every point of network path between the sender and receiver as stated in [3]. If we think about these two facts, the first idea is to create secure applications which can guarantee appropriate security level in the highest OSI/ISO layer – application layer. There is a question: what about existing unsecured applications?

[2)] DoS attack – denial-of-service attack is an attempt to make a some device unavailable to its intended users.

Encryption process requires some hardware resources like higher CPU and memory usage. Moreover some information – like funny, entertainment web pages with jokes or news portals – does not have to be encrypted. The basic purpose of IPsec protocol is to provide some security standards in 3rd and 4th layers. This protocol can be used in two modes. First of them is a transport mode and second one is called tunnel mode. The different is that transport mode puts additional header between TCP and IPv4 headers or adds additional header to IPv6 packet and tunnel mode encapsulates whole IPsec packet in another IP packet. The big disadvantage of IPsec is that because of performance requirements, only symmetric algorithms can be used. IPsec allows using any encryption mechanism including null algorithm[3]. Perhaps it would be good to implement Diffie-Hellman algorithm to establish session key. ISAKMP and IKE protocols which are used for key exchange has few well know vulnerabilities, so key exchange process is not secure.

IPsec can add two types of headers to TCP/IP packets. First of them, Authentication Header does not allow for encryption, but provides mechanisms for integrity control and protection against repeated attack. This header can be used only in transport mode or as an additional header in IPv6 packet. Second header – Encapsulation Security Payload can be used in both modes and allow for encryption. Both headers can check data integrity using HMAC (Hashed Message Authentication Code) method. This method counts a hash value for whole message and key. The difference between AH and ESP headers is that AH checks also integrity of many (but not all) fields from IP header like IP addresses (some fields like TTL[4] can't be verified).

## 6. Wireless networks

Some, physical aspects of wireless networks have been just described at the begin. However, algorithms and encryption mechanism have not been discussed yet. It is much more difficult to limit access to wireless signal than to the network cable. Therefore it is important to apply other security mechanisms to IEEE 802.11 wireless networks. "Wired Equivalent Privacy" protocol was a first protocol used for protection network in 802.11 standard (Fig. 2). The name of this protocol suggests that it should provide security level similar to wired, cable networks. The truth is that this is a weak protocol. The protocol was designed in 1997 year and uses RC4 algorithm. The 2nd fact is that David Wagner discovered first RC4 vulnerabilities 2 years earlier. The WEP protocol can use 40 or 104-bits key. At the begin CRC32 checksum is counted and concatenated to clear-text message. Then Initialization Vector (IV) is concatenated with a key and it gives the seed for RC4 algorithm. IV and encrypted message are sent over the network.

---

[3] In this case there is no encrypton.
[4] TTL (Time To Live) is decremented in every router.

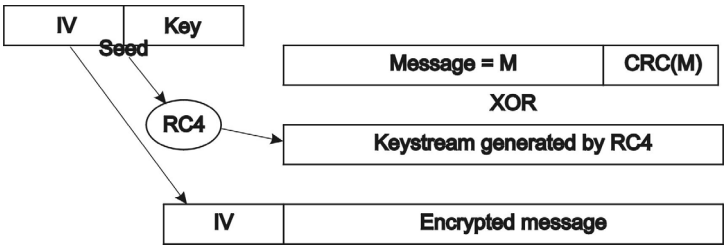


**Fig. 2.** The idea of WEP protocol

Keys used in WEP are not so long, especially 40-bit keys. Packets encrypted by such keys can be cracked by brute-force method using Tim Newsham optimization. His method reduces the 40-bit key space down to 21 bits. Second problem with WEP is key stream reuse. If two ciphertexts were XORed with the same key stream, this key stream can be eliminated using equation (1).

$$(P_1 \mathit{XOR} \text{RC4(seed)}) \mathit{XOR} (P_2 \mathit{XOR} \text{RC4(seed)}) = P_1 \mathit{XOR} P_2 \tag{1}$$

If some bits of P1 message are known, the same bits from P2 can be easily recovered. Initialization Vector is only 24-bits long, so it is probable that it will be reused after some, short time. Moreover, the standard does not specify how to choose and generate IV for next packets. Next vulnerability of WEP is connected with CRC32 function. This function is enough for casual error detection, but from cryptographic point of view is not secure. It is known that the intruder can exchange some bits of message and then some bits of CRC function in that way that CRC will be still correct. The most popular attack against WEP is Fluhrer, Mantin and Shamir (FMS) attack, descried in [1]. This attack takes advantage of using initialization vectors and weaknesses of key generation in RC4. It is well described attack and popularized by many network tools. The last attack, very effective in many situations is a dictionary attack. Many times WEP key is equal to SSID or is a short, simple word.

Is it possible to prevent against such attacks? Some of described attacks can be prevented by using Dynamic WEP with one of EAP protocols (Extensible Authentication Protocol) like EAP-TLS or EAP-TTLS. Both methods allow for safe authentication and key exchange. Basically, EAP is not a single protocol, but it is an authentication framework. It is a set of common functions and negotiation mechanisms. One of advantages of Dynamic WEP is a fact that new key is generated and propagated in network, once per few minutes. It should be too short time to crack existing, current key. However this idea does not provide very high security level.

Next, much more secure resolution for wireless networks are WPA and WPA2 protocols (WiFi Protected Access). Both can work with RADIUS server (Remote Authentication Dial In User Service) (Fig. 3). Both protocols can also work in two modes: as WPA Personal or Enterprise. Personal versions uses “Pre Shared Key”, Enterprise uses RADIUS and EAP protocol. The disadvantage of PSK method is that the secret key is shared with all network

users. RC4 algorithm is replaced by TKIP, AES or CCMP in WPA protocols. TKIP (Temporary Key Integrity Protocol) implements three additional security features: mixing function for key and initialization vector, sequence counter against replay attack and 64-bit integrity check function, named MICHAEL. AES (Advanced Encryption Standard) is a well know secure algorithm. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is based on AES and allow for message integrity checking. To sum up, WPA2 protocol is the most secure protocol for wireless network, however the most dangerous thing is PSK mode and dictionary attack for a secret key in this mode. Good comparison of existing WiFi protection methods is in [6].

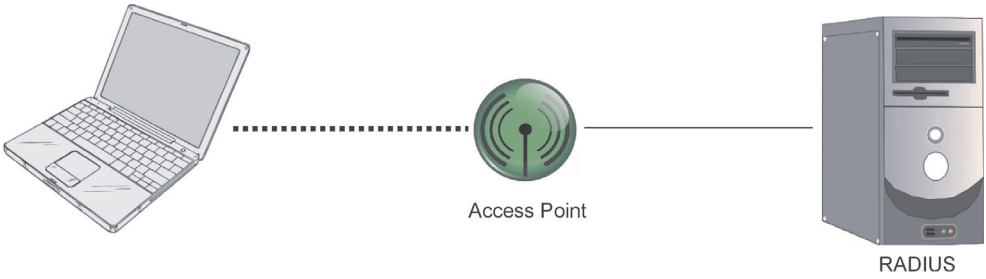


**Fig. 3.** Wireless network with RADIUS server

## 7. Perspectives – what can be done for security?

I have tried to review security mechanisms and insecure resolutions in few popular, low-level protocols. I think that we can draw the conclusions from described solutions and learn how to design secure protocols in the future and what can be dangerous in some of them. Table 1 contains described network vulnerabilities and some good advices how to protect against attacks which utilizes such bugs.

The author is working on some guidelines which can be used for existing and new protocols. Knowledge and security experiences in existing protocols are very important and useful. First of all we should analyze existing protocols, protection and security mechanisms, existing bugs, faults and vulnerabilities. The second step is to gather all this things together and then to start formalization process. There are many guidelines and tutorials how to create a secure programs, but even huge number of such things does not guarantee that software is or will be secure. I strongly believe that wrong, unsecured protocols can cause faults in software. Sometimes protocols forces damageable resolution in created software. For example if protocol requires clear text password for authentication, the application cannot be secure. There are a huge number of specific protocols designed only for specific purposes and used by small group of people. Therefore I see the reason of analyzing and creating guidelines for secure protocols.

**Table 1**
Vulnerabilities and protection methods

| Vulnerability | Protection method |
|---|---|
| Sniffing | splitting network to as small as possible collisions domains<br>using cryptography and encryption algorithms |
| Spoofing | using authentication mechanisms<br>putting sequence numbers in packets and counters<br>on destination hosts |
| ARP poisoning | pre-configured ARP tables (without network requests<br>and responses)<br>IPv6 and auto-configuration mechanism<br>broadcasting ARP responses |
| DHCP DoS | static IP configuration, without DHCP |
| Wrong offset and sequence numbers in IP header | precise specification of protocol, what to do in such situations.<br>Programmers should not decide about fault management<br>in protocol |
| Symmetric key attack (IPsec) | using algorithms with public and private keys |
| Weaknesses of used algorithms | allowing for choosing few algorithms – like in IPsec |
| Brute force attack (IV in WEP) | using longer values<br>choosing strong cryptographic algorithms |
| Shared key (WEP, WPA) | using RADIUS server instead of PSK |

## References

[1] Erickson J., *Hacking – The Art of Exploitation*. No Starch Press, San Francisco 2003.
[2] Howard M., LeBlanc D., Viega J., *The 19 Deadly Sins of Software Security*. McGraw-Hill/Osborne, California 2005.
[3] Tanenbaum A.S., *Computer Networks* (4th Edition). Prentice Hall, New Jersey 2003.
[4] Menezes A.J., van Oorschot P.C., Vanstone S.A., *Handbook of Applied Cryptography*. CRC Press 1996 (online version).
[5] Ogiela M.R., *Security of computer systems*. Wydawnictwa AGH, Kraków 2002 (in Polish).
[6] T*he Top 10 Most Critical Internet Security Threats*. (2000–2001 Archive) – http://www.sans.org/top20/2000/.
[7] Security Technical Guidelines from DISA – http://iase.disa.mil/stigs/stig/index.html.
[8] Ogiela M.R., Ogiela U., *Linguistic Cryptographic Threshold Schemes, IJFGCN*. International Journal of Future Generation Communication and Networking, vol. 2, No. 1, March 2009, 33–40.
[9] Ogiela M.R., Ogiela U., *Linguistic Extension for Secret Sharing (m, n)-threshold Schemes*. 2008 International Conference on Security Technology, December 13–15, 2008, Hainan Island, Sanya, China, 125–128, ISBN: 978-0-7695-3486-2, DOI: 10.1109/SecTech.2008.15.
[10] *IANA port numbers.* http://www.iana.org/assignments/port-numbers.