HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Tibor Szabó
szabo.tibor@nbsz.gov.hu

NETWORK SECURITY PROBLEMS ON LAYER 2

Abstract

IT, communications equipment and systems - that are part of the critical infrastructure components - communicate with each other over the Internet and are available to anyone anywhere in the world, and thus become the target of attacks. The method of attack is usually infected documents, malicious emails, Trojan programs, but less is said about the cases of attack of Layer 2. As a result, even between the professionals we can find someone who is just focusing on the security of the device itself and not on the security of the management system during the implementation of the information security, the data elements are omitted. According to experience, I need to draw your attention to some security problems of the Layer 2, when those are ignored, it can increase the vulnerability of the critical infrastructure, including the information systems and the national security systems.

Az informatikai, a kommunikációs eszközök és rendszerek - melyek részei a kritikus infrastruktúrát alkotó rendszerelemeinknek – kommunikálnak egymással az interneten és elérhetőek a világ bármely pontjáról bárki számára, ezáltal támadások célpontjává válhatnak. A napi sajtóban látott támadások módszerét tekintve többnyire fertőzött dokumentumokról, kártékony email tartalmakról, rosszindulatú trójai programokról értesülünk, azonban kevesebb szó esik azokról az esetekről, amikor Layer 2 szinten történik a támadás. Ennek hatására még a szakemberek között is található olyan, aki informatikai biztonság megvalósítása során az adatokat kezelő rendszerelemek közül kihagy néhányat és magára az eszközrendszerre koncentrál és azon törekszik csak a biztonság megvalósítására. Tapasztalatok alapján szükségesnek tartom cikkemmel felhívni a figyelmet néhány olyan Layer 2 szintű biztonsági problémára, melyek figyelmen kívül hagyása növeli kritikus infrastruktúráink, információs rendszereink sebezhetőségét beleértve a nemzet biztonsága szempontjából fontos rendszereket.

Keywords: *layer 2, spanning tree protokoll, VLAN támadás, MAC cím tábla, Wi-Fi, ~ DHCP starvation attack, CAM table, MAC spoofing, 802.1q*

INTRODUCTION

Day by day we can read news about hackers who attacked banks, various diplomatic missions, government portals, research institutes, airports or taken relevant information from oil companies. Nowadays such events are more and more frequent, because – it is well known - that the IT and communications equipment and systems became part of our lives. At home, at work, on the way, even while doing the housework we use them.

In addition, it is more and more usual to entrust to them such functions like perception, control. They are available from anywhere in the world and they communicate with each other through telecommunication or local connections. Those equipment and systems can be available with few clicks. All these features make our daily life more convenient, but it can cause risk to us, to the institutions and to our country - thinking on the critical infrastructures, which are also a popular target for the attackers. [1], [2]

The method of attack is usually infected documents, malicious emails, Trojan[1] programs, but less is said about the cases of attack of Layer 2[2]. As a result, even between the professionals we can find someone who is just focusing on the security of the device itself and not on the security of the management system during the implementation of the information security, the data elements are omitted. [5]

According to experience, I need to draw your attention to some security problems of the Layer 2, when those are ignored, it can increase the vulnerability of the critical infrastructure, including the information systems and the national security systems.

Because the Layer 2 attacks are relatively more difficult to accomplish from outside, from the Internet, they are only concentrate on the other layer of OSI[3], they think that the LAN[4] and the backbone network provided by the internet service provider is safe, but it isn't. There are some well-known technics which allows reaching the elements of the LAN network in short time from outside: For example: Backdoor[5], Wi-Fi[6] hacking[7].

LAYER 2

Before explaining the vulnerabilities of the Layer 2, please find below a few words about what is this – for those who are less experienced in this field.

The Layer 2 is one part of the OSI – seven-layer hierarchical – model. The ISO (International Organization for Standardization) developed the OSI model, so that they can determine the requirements of mutual cooperation the communication devices – including computers – between each other with individual layers. In fact, the same communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it. Main concern was that the different manufacturer's products (hardware, software) work together at the border of different layer.

Find below the list of levels with short explanation: (Figure 1.)

---

[1] Trojan is a type of malware which appears to perform a desirable function but instead prepare an unauthorized access to the user's computer. [4]

[2] The Layer 2 (data link layer) is one part of the OSI model. It will be explained below in more detail.

[3] Open Systems Interconnection model is an abstract reference model of networking. [3]

[4] Local Area Network is a computer network that connects computer in a limited area. This area can be extended with special equipment.

[5] Backdoor is a method of bypassing normal authentication, securing illegal remote access to your computer. [6]

[6] Wi-Fi is a popular technology that allows an electronic device to exchange data via radio waves based on IEEE (Institute of Electrical and Electronics Engineers) standards. [7]

[7] In this context, the activity in which hacker seeks and exploits a computer or computer network weaknesses (in this case the Wi-Fi).

Figure 1. OSI Reference Model [16]

The names of the individual layers are obvious, but please find below few explanation to obtain a more complete picture about the function of the layer.

The *physical layer* defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or fiber optical cable. The major functions and services performed by the physical layer are: Establishment and termination of a connection. Modulation or conversion between the representations of digital data in equipment.

The layer we are interesting in is the *datalink layer* provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. Following are the functions of data link layer:

- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control
- Media Access Control (MAC)

The *network layer* provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (remember to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer.

The *transport layer* provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

The *session layer* controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application.

The *presentation layer* establishes context between application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. (for example: MIME[8] decoding.)

The *application layer* is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component.

[8] Multipurpose Internet Mail Extensions - is an Internet standard that extends the format of email to support: Text in character sets other than ASCII, Non-text attachments, Message bodies with multiple parts, Header information in non-ASCII character sets. [9]

ATTACK TECHNIQUES

The attack techniques on Layer 2 can be so efficient and "invisible", because there is a fundamental problem in the OSI model which was built to allow different layers to work without knowledge of each other and the information flows up and down to the next subsequent layer as data is processed. If one layer is hacked, the communications are compromised without the other layers being aware of the problem. In this case the Layer 3 and Layer 1 will not be aware if Layer 2 is attacked. (Figure 2.) [10] [11]

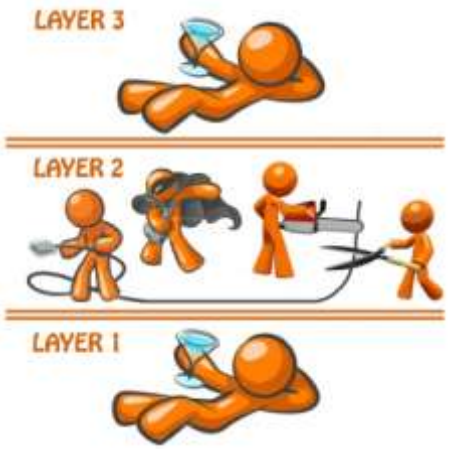

Figure 2. Layer 2 is attacked

There are three main classes of attacks:

- Spanning Tree Protocol
- Cisco VLAN[9]/Trunking Protocols
- Other attacks[12]

Spanning Tree Protocol

Spanning-Tree Protocol (STP) prevents loops from being formed when switches[10] or bridges[11] are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU[12] messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is only one active path between two network devices. [13] Within this framework the bridges negotiate between them, who will be the „root" bridge in the network, determine the least cost paths and disable all other paths.

The attack technique of this protocol, the *Spanning Tree Protocol manipulation attack*, within this framework the attacker sends BPDUs to become „root" bridge (or switch) in the network. Therefore the attacker can influence the flow of data. Requires attacker is dual homed to two different bridges (or switches) or one of the two connections is WLAN[13] access point which is not connected to the same bridge (or switch).

[9] Virtual LAN: A VLAN has the same attributes as a physical LAN. One network cable can have more grouped VLANs on the same network switch port (interface). [15]
[10] Switch is a computer networking device that links network devices.
[11] A bridge is a device which connects two parts of a network together at the data link layer (layer2).
[12] Bridge Protocol Data Unit: When STP is enabled, bridges send and receive spanning-tree frames, called BPDUs, at regular intervals and use the frames to maintain a loop-free network. [14]
[13] Wireless LAN

Attacker can eavesdrop all messages of victims; he can inject new ones in MITM[14] position. (Figure 3.)

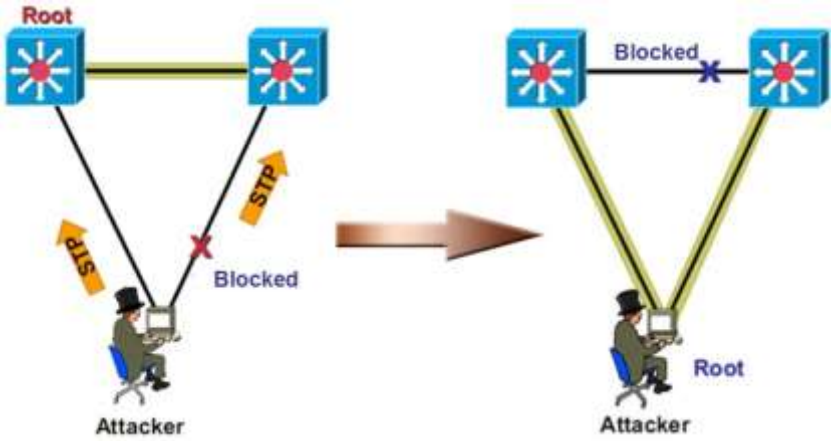

Figure 3. Spanning Tree Protocol manipulation [10]

Cisco VLAN/Trunking Protocols

VLAN's allow a network manager to logically segment a LAN into different network of departments such as marketing, sales, accounting, and research. There are lots of VLANs over the backbone switches of Internet connecting different site of company. The attacker has two method of *VLAN hopping attack* in order to be a member of other VLANs:

1. Basic VLAN hopping attack:The switches connected to a trunk[15] link, which has access to all VLANs by default. The attacker station can spoof as a switch with DTP[16] signaling, and the station will be a rogue switch – member of all VLANs and all traffic can be monitored. The „Yersinia" software is very useful for this task. (Figure 4.)

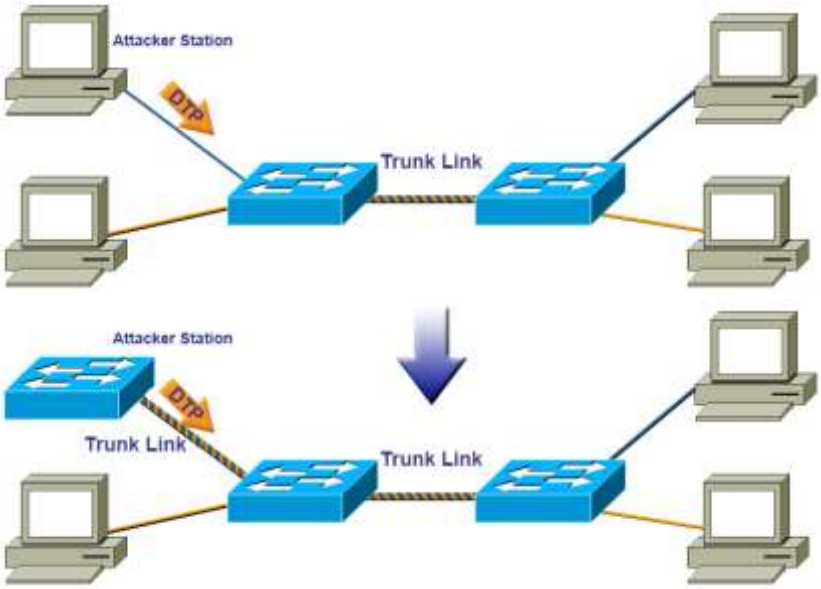

Figure 4. Basic VLAN hopping attack [10]

[14] Man-in-the-middle
[15] It is used to route traffic for multiply VLANs across the same physical link.
[16] Dynamic Trunk Protocol: Automates (802.1q/ISL) trunk configuration and operates between switches. DTP usually enabled by default. 802.1q is the networking standard that supports VLANs on an Ethernet network. ISL is a Cisco proprietary protocol that maintains VLAN information.

2. Double tagging VLAN hopping attack*:*A widely used VLAN networks operate with an additional 802.1q header, or VLAN tag to distinguish the VLANs. VLAN tag changes the information frame. The service-provider infrastructures are double-tagged, with the outer tag containing the customer's access VLAN ID, and the inner VLAN ID being the VLAN of the incoming traffic. When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the packet is processed inside the switch. The attacker sends „Double tagging" frame. The first belongs to the own VLAN and the second one belongs to the target VLAN. The switch performs only one level decapsulation (strip off first tag) and the attacker can use unidirectional traffic to the Victim. This method works if trunk has the same VLAN as the attacker and the trunk operates with 802.1q. (Figure 5.) [10]

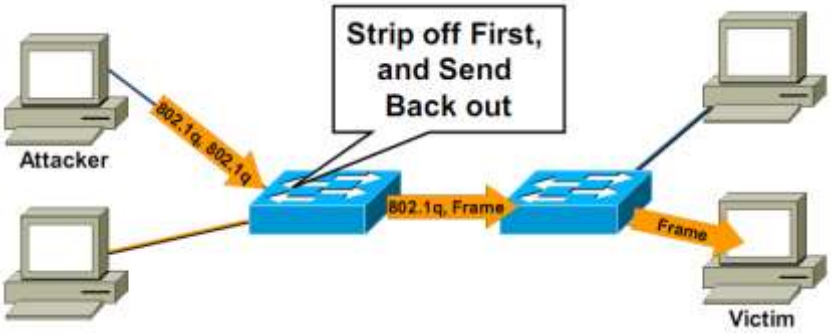

Figure 5. Double tagging VLAN hopping attack [10]

Other attacks

In this section, only those relevant attack techniques will be explained - in addition to the previous ones - which are widely known and worth considering at the developing of the system-wide security policy and at work out of the basic safety procedures.

Cisco Discovery Protocol (CDP) attack

The Cisco Discovery Protocol (CDP) is a proprietary protocol that all Cisco devices can be configured to use. CDP discovers other Cisco devices that are directly connected, which allows the devices to auto-configure their connection in some cases. CDP messages are not encrypted. Most Cisco routers[17] and switches have CDP enabled in the default configuration.

Can be used to learn sensible information about the CDP sender (IP address[18], Cisco IOS[19] software version, router model, capabilities...).

Besides the information gathering benefit CDP offers an attacker, there was vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets.

CDP is unauthenticated: an attacker could craft bogus CDP packets and have them received by the attacker's directly connected Cisco device. (Figure 6.) If the attacker can get access to the router via Telnet, he can use the CDP information to discover the entire topology of your network at Layer 2 and 3, and he could launch a very effective attack against your network.[10], [17]

[17] A router is a device that forwards data packets between computer networks. A router is connected to two or more data lines from different networks.

[18] Internet Protocol address is a numerical label assigned to each device (e.g. computer, printer) in a computer network. [18]

[19] Internetwork Operating System is software used on most Cisco Systems routers and switches.

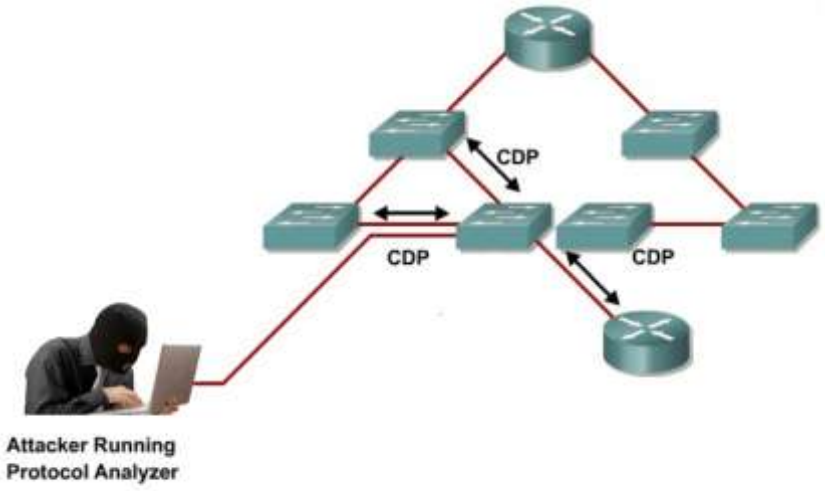

Figure 6. CDP attack

CAM[20] table overflow attack

Widely used Cisco switch models use the CAM table, which stores information such as MAC[21] addresses available on physical ports. CAM tables (sometimes called MAC address table) have a fixed size (19KB...128KB, it can store about 100…100000 MAC entries).

When frames arrive on physical ports, the source MAC addresses are learned from Layer 2 packet header and recorded in the CAM table. All entries have a default aging timer which is 300 seconds. If a host does not send frames toward the port, the entries will be removed after 5 minutes.

The switch forwards the frame to the MAC address port designated in the CAM table. If the MAC address does not exist, the switch acts like a hub[22] and forwards the frame out every other port on the switch.

There is a common tool that performs CAM overflow. This tool can generate 155000 MAC entries on a switch per minute. A CAM overflow attack turns a switch into a hub, which enables the attacker to reach every host on the network, to eavesdrop on a communication and perform MITM attacks. This method is applicable to attack the neighbor switches. (Figure 7.) [10]

[20] Content Addressable Memory

[21] Media Access Control - is a unique identifier assigned to network interfaces for communications on the physical network.

[22] Hub is a device for connecting multiple Ethernet devices together. A hub works at the Layer1 If a frame introduced at one port appears at every another port.

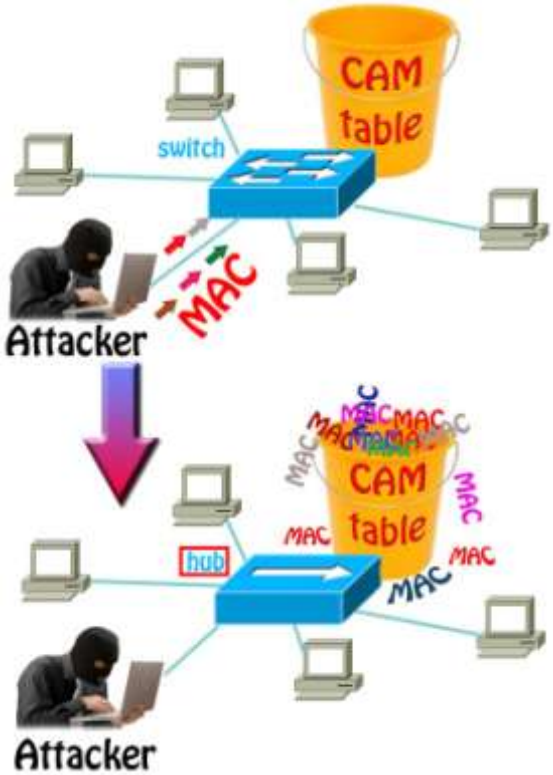

Figure 7. CAM table overflow attack

MAC Spoofing (ARP[23] poisoning)

How many people think that to see the ARP packets on your own computer? Everybody can answer to this question differently.

MAC spoofing attacks are launched by attacker on a Layer 2 network. The attacker can send out a gratuitous ARP (GARP) to the network. GARP is used by hosts (computers) to „announce" their IP address to the local network and avoid duplicate IP addresses on the network. Computers, routers and other network hardware may use cache information gained from gratuitous ARPs. Because ARP has no methods for authenticating ARP replies on a network, ARP replies can come from other system which is expected.

In one common attack the attacker says „my PC is the default gateway" so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway so that victims do not notice any change in their network access. An attacker on a fast enough host can capture the traffic and can modify them. Figure 8. [10]

[23] Address Resolution Protocol is a request and reply protocol. It is used to map of MAC address to IP address.

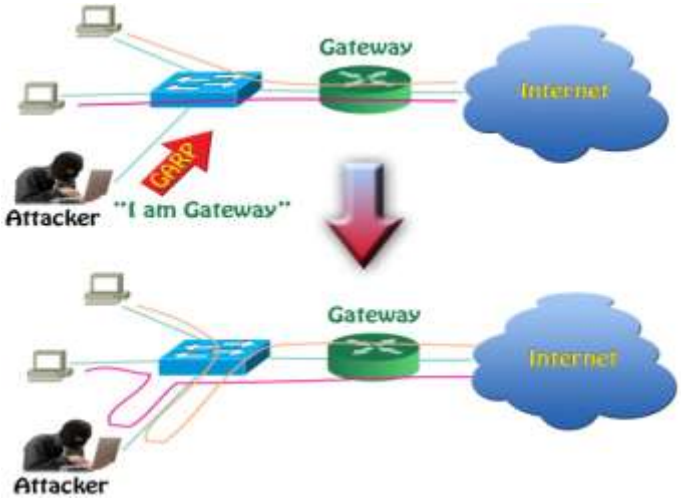

Figure 8. MAC Spoofing

DHCP[24] starvation attack

The DHCP server is used to configure network devices so that they can communicate on computer network. The clients and a server are operating in a client-server model. DHCP client sends a query requesting necessary information (IP address, default gateway[25], and so on) to a DHCP server. On receiving a valid request, the server assigns the computer an IP address, and other IP configuration parameters.

This is special kind of attack where attacker sends tons of requests to the DHCP server with a false MAC address. If enough requests flooded onto the network, the attacker can completely exhaust all of the available DHCP addresses. Clients of the victim network are then starved of the DHCP resource

The network attacker can then set up a Rogue DHCP Server on the network and reply modified IP configurations to the victims. (Figure 9.) These parameters ensure the MITM possibilities to the attacker. [10]

Figure 9. DHCP starvation attack

[24] Dynamic Host Configuration Protocol is a network protocol.

[25] Typically is a router on a computer network that serves as an access point to another network (e.g. public internet)

Wireless 802.11[26] (Wi-Fi) attack

Everyone is familiar with the Wi-Fi networks. Wi-Fi can be less secure than wired (ethernet) connections because an attacker does not need a physical connection, since only need one antenna and a laptop to compromise one.

In this type of attack, the attacker can execute:

- to insert himself in the MITM position (client's data can be modified,
- to deny the service,
- to capture all traffic.

In order to insert oneself in the middle of the communication, one has two possibilities:

- Send deauthentication packets to one or more clients which are currently associated with an AP and set up a rouge AP with the same credentials as the original for purposes of allowing the client to connect to it.
- Set up a rouge AP with a big signal (bigger than the original) and same credentials as the original for purposes of allowing the new client to connect to it.

The subject of another article could be: how can we access the security protocol of Wi-Fi.

In order to deny service there are two possibilities:

- There are several commercial devices available today that can bring down the wireless LAN with a lot of noise at wireless operation frequency.
- The affected AP can be rejected that user access by flooding network traffic.

In order to capture traffic of victim with network interface card, there are two possibilities (even from huge distance):

- Card is used in normal mode.
- Card is set up in monitor (promiscuous[27]) mode. [7], [19], [20]

5. CONCLUSIONS

This article is an overview of the most well-known attack techniques on Layer 2 and draw attention to the vulnerabilities of this level emphasizing that the other layers being aware of the problem. A lot of attention is paid to securing the higher layers of the OSI reference model with network-level devices such as firewalls, intrusion protection systems (IPS), and applications such as antivirus and host-based intrusion protection (HIPS).

The attacker can

- eavesdrop traffic,
- manipulate data,
- deny the information flow, and
- use combination of the above mentioned.

Apply any of these options pose a serious threat to critical infrastructure, state institutions or governmental systems, even if no attacking intent is used. Certain critical infrastructure is controlled via the Internet which is maintained by wired and mobile telecommunication carriers.

[26] Wireless communication protocol on Layer 1 and Layer 2.

[27] Promiscuous mode is a mode for a wired network interface controller or wireless network interface controller. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

Transmission of the information is important to emphasize, as also can cause disaster. For example, the control information cannot reach to endpoints due to unavailability of service. The attacker is easy to achieve this position. For instance powerful jamming equipment is used in wireless or mobile technology. In view of the rapidly developing technology background of Wi-Fi area, where the marketed devices already have 7Gbps data transmission speeds at the end of year and one of the dominant mobile manufacturer's vision of the mobile transmission, you can easily see that the data flow will significantly rise. [8], [21]

In addition these methods are mentioned in the article are likely to access IDs and passwords, which is also threat. Of course, the attack techniques are known by manufacturers and they do everything to mitigate them. For example Cisco implemented a technology into IOS called Port Security that mitigates the risk of a Layer 2 CAM overflow attack.

The above mentioned attacks can be used in only certain settings, therefore it should be mentioned the human factor, which plays a key role in the development and operation of those devices. This topic is worth a detailed another article.

In order to eliminate these attack techniques protection of LAN networks of critical infrastructures must be improved. The government should make a laws, which placed in a position of law enforcement and military organizations, which provide greater suasion over the security of telecommunications networks.

In summary we must be prepared to mitigate the methods of attacks when implementing security systems of critical infrastructure on all levels (including Layer 2) of OSI model.

References

[1] GReAT, Kaspersky Lab Expert: The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies (2013.01.14.)

[2] MTI: Hackerek támadták meg az Európai Bizottságot http://www.origo.hu/nagyvilag/20121110-hackerek-tamadtak-meg-az-europai-bizottsagot-azerbajdzsanban.html (2013.01.14.)

[3] OSI model, http://en.wikipedia.org/wiki/OSI_model (2013.01.12.)

[4] Trójai program, http://hu.wikipedia.org/wiki/Tr%C3%B3jai_program (2013.01.12.)

[5] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana (BOLYAI SZEMLE XVII. évf. 4., 2008)

[6] Backdoor computing, http://en.wikipedia.org/wiki/Backdoor_%28computing%29 (2013.01.16.)

[7] Wi-Fi, http://hu.wikipedia.org/wiki/Wi-Fi (2013.01.16.)

[8] Samsung Exynos 5 Octa & Flexible Display at CES 2013 Keynote http://www.youtube.com/watch?v=GDJ67df0p6A&feature=player_embedded (2013.01.15.)

[9] MIME, http://en.wikipedia.org/wiki/MIME/ (2013.01.16.)

[10] Sean Convery, Cisco Systems: Hacking Layer 2: Fun with Ethernet switches http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (2013.01.18.)

[11] Yusuf Bhaji, Cisco Systems: LAYER 2 ATTACKS & MITIGATION TECHNIQUES http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.pdf (2013.01.21.)

[12] Enno Rey Lead Auditor, ERNW GmbH: Network Security on OSI Layer 2 and 3 http://pdfsb.com/readonline/62464a4c65677431586e522b4348706b55513d3d-4366147 (2012.10.04)

[13] Spanning Tree Protocol http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html (2013.01.19)

[14] Wifi Glossary OL-7080-01 http://www.cisco.com/en/US/docs/wireless/access_point/1300/12.3_7_JA/configuration/guide/b37glos.pdf (2013.01.22)

[15] Virtual LAN, http://en.wikipedia.org/wiki/Virtual_LAN (2013.01.18)

[16] How NAT Works, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a008009484831.shtml (2013.01.17)

[17] Common Switch Securitty Attacks- CDP and Telnet Attacks http://ccnaanswers-khim.blogspot.hu/2011/05/common-switch-securitty-attacks-cdp-and.html (2013.01.23)

[18] IP address, http://en.wikipedia.org/wiki/IP_address (2013.01.12)

[19] SANS Institute: Understanding Wireless Attacks and Detection: http://www.sans.org/reading_room/whitepapers/detection/understanding-wireless-attacks-detection_1633 (2013.01.23)

[20] Ec-Council,Course Technology: Ethical hacking and Countermeasures Courseware volume 4. page 2124-2254.

[21] Jön a 7 Gbps-os WiFi http://www.sg.hu/cikkek/94678/vezetek_nelkuli_atvitel_hd_eszkozokre/ (2013.01.16.)