SOLUTIONS FOR SECURITY ENHANCEMENTS IN DIGITAL NETWORKS

Bogdan GOHOREANU, Florin SANDU, Dan-Nicolae ROBU

"Transilvania" University, Brasov, Romania (bogdan.gohoreanu@gmail.com, sandu@unitbv.ro, robu.dan@unitbv.ro)

DOI: 10.19062/2247-3173.2017.19.1.44

Abstract: *The paper is approaching a subject that is sensitive nowadays - security vulnerabilities and protection methods that can be implemented to prevent a cyber-attack. In this scope, we studied Telnet and SSH network protocols using Wireshark and made a comparative assessment regarding the safety mechanisms that each has when the data is transmitted. We proposed security enhancements dedicated to Wireless Networks because they are very popular these days and it is well known the specific high risk of a security breach. In the Internet applications sphere there are presented the most known security breaches and there are proposed some methods to fight against them.*

Keywords: *security, digital communication networks, web applications, network protocols, SQL Injection*

1. INTRODUCTION

Considering the technology progress, cyber security is an area which is developing fast. The big companies and government institutions are investing more and more resources in network security. Training their employees to identify cyber-attacks is an important part of this process.

This domain is continuously growing, involving major changes in a short time because the attackers are very inventive and the traditional preventive methods do not give efficiency always as expected. This kind of problems causes financial loses in amount of billions of dollars and the average cost of a security incident is about $12 million. Every year, the authorities have knowledge about millions of cyber-attacks, some of them being successful, but others not so much [1].

2. SECURITY ASPECTS IN DIGITAL NETWORKS AND WEB APPLICATIONS

2.1 Network Protocols

Considering the importance of working "remotely" nowadays, this paper is presenting the main advantages and disadvantages of the Telnet protocol and which is the alternative solution that satisfies also the security criteria – the SSH protocol.

Telnet is a protocol used for remote connection to a server. Client – server connections are established using the TCP protocol. After this stage, Telnet server and client are negotiating the resources that will be supported by each of them during the connection [2].

This protocol doesn't have security mechanisms for data transmission and that is why all information is transmitted in plain text, including passwords [3]. Another safety measure that is not implemented is authentication and the consequence can be communication interception and changing the source computer with another that is pretending to be the real source.

Another protocol that is serving the same purpose as Telnet, but doesn't have obvious security vulnerabilities is SSH (Secure Shell). Using SSH, data is encrypted and for authentication this protocol is using a public key [4].

A domain that is continuously developing nowadays is IoT (Internet of Things) and one of the standard protocols is MQTT (Message Queueing Telemetry Transport). Secure communications can be implemented by using MQTT [5]. MQTT implementations provide a security certificate mode that can be achieved with the Java Paho library [6, 7].

2.2 Web Applications

Statistics show that 61% of the USA companies are the target of "web-based" attacks. This type of attacks is motivated by the current state of web applications: 55% have at least one high severity vulnerability, 84% have at least one medium severity vulnerability and 35% of the web-sites have certificates based on SHA-1 [8].

The main "web-based" threats are:

- Brute Force Attack;
- Malware – Spyware/Key logger;
- SQL Injection;
- Social – Phishing.

The most known, but still present in 25% of the cases is SQL Injection. A type of SQL Injection can be altering the Connection String parameters.

Connection Strings are used to connect the application with the database.

E.g. connectionString = "Data Source=ServerName;Initial Catalog=DataBaseName;User Id=Username; Password=pwd";

SQL Injection consequences:

- Loss of data confidentiality;
- Loss of data integrity;
- Data loss;
- Compromise the entire network.

Methods to prevent SQL Injection [9]:

- Using Firewall to filter malicious data;
- Using reduced privileges accounts for database connections - administrator account to be used if necessary;
- Using parameterized queries or stored procedures instead of dynamic SQL.

2.3 Wireless Networks

Wi-Fi networks are very popular nowadays because the majority of people installed this type of Internet home connections.

The main Wi-Fi advantages:

- Low cost;
- Easy to deploy;
- Radio technology with high performance that doesn't depend on the building physical parameters.

These characteristics are also big vulnerabilities. In case of an attack on this type of network the attacker is very difficult to be found. Main types of attacks that can happen are the following:

- Brute Force Attack on the AP password;
- WEP/WPA key crack;
- "Denial of Service" attack;
- "Man-in-the-middle" attack.

There are Linux distributions (e.g. Kali Linux) that are more suitable to test attacks on the wireless networks. The following two programs are popular for testing network security: Reaver and Pixiewps. An attacker can be focused to crack the WPS, rather than the WPA key. If a device will connect via WPS, it will receive also a WPA key.

3. PRACTICAL SOLUTIONS AND EXPERIMENTAL VALIDATIONS

3.1. Telnet security vulnerabilities

Network protocols security was tested using Wireshark by capturing data packets sent when connecting to a remote server from a computer running the Windows 7 operating system.

It can be seen in the screenshots of Fig.1 that, using Telnet, the information is being sent in plain text. Even login credentials (username and password) are transmitted in plain text ("password: 123").

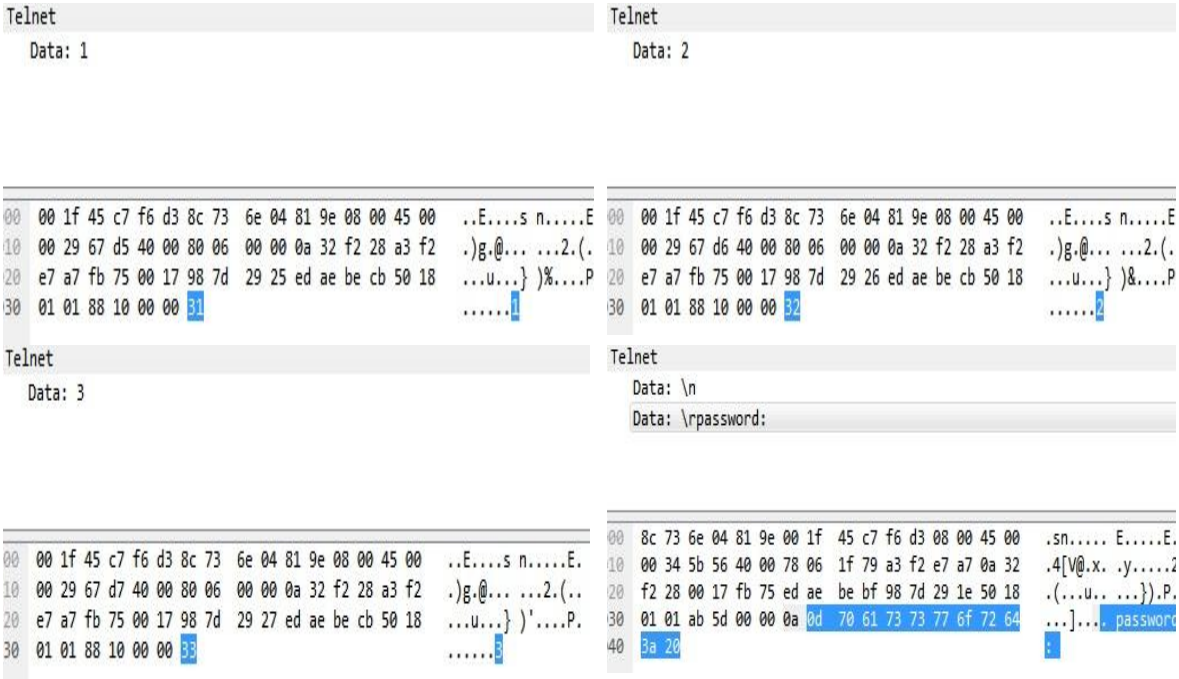

FIG. 1. Telnet packets - data transmitted in plain text

3.2. SQL Injection

Most of the sites give users the possibility to subscribe for receiving newsletters via e-mail. We have proven specific site vulnerabilities by programming an example of a wrong subscribing form (Fig.2).

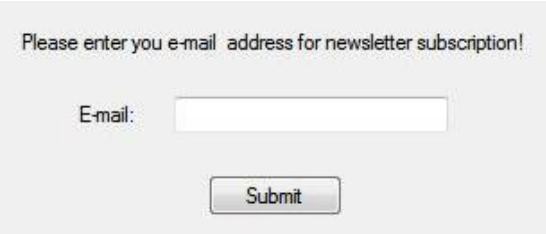

FIG. 2. Example of subscribing form

Such an application is vulnerable to SQL Injection because of the form processing. Saving the e-mail address in the database is done using the following C# code:

```
private void btnSubmit_Click(object sender, EventArgs e)
{
string queryString = "insert into table_name values('" + textBoxEmail.Text+"')";
SqlConnection connection = new SqlConnection(connectionString);
SqlCommand command = new SqlCommand(queryString, connection);
command.Connection.Open();
command.ExecuteNonQuery();
}
```

Instead of a valid e-mail address, an attacker can enter the following text that will be interpreted as an SQL command and executed:

user1@domain.com');insert into newsletter values('user2@domain.com

As a consequence, in the database there will be introduced two e-mail addresses: user1@domain.com and user2@domain.com

These types of mistakes are developer's faults. In the above-presented case, the consequences do not have a vital impact, but it can be introduced malicious code that will affect the functionality of the application (e.g. removing the database).

This kind of breach can be fixed in several ways:

- Introducing code to validate the format of an e-mail address;
- Using a parameterized stored procedure for database insertion.

3.3. Securing the Wireless Networks

For a better securing of wireless home networks, it exists the possibility to hide the network name or, in technical terms, the network SSID. By doing this, the network will be invisible to a potential attacker.

The majority of wireless routers used for home Wi-Fi can be configured very easily to hide the SSID. The steps for doing this configuration on a TP-Link router are the following: the user opens an Internet browser and connects to the router using its web interface; in the section "Wireless > Wireless settings" he/she will deactivate the option "Enable SSID Broadcast" (Fig. 3) [10].

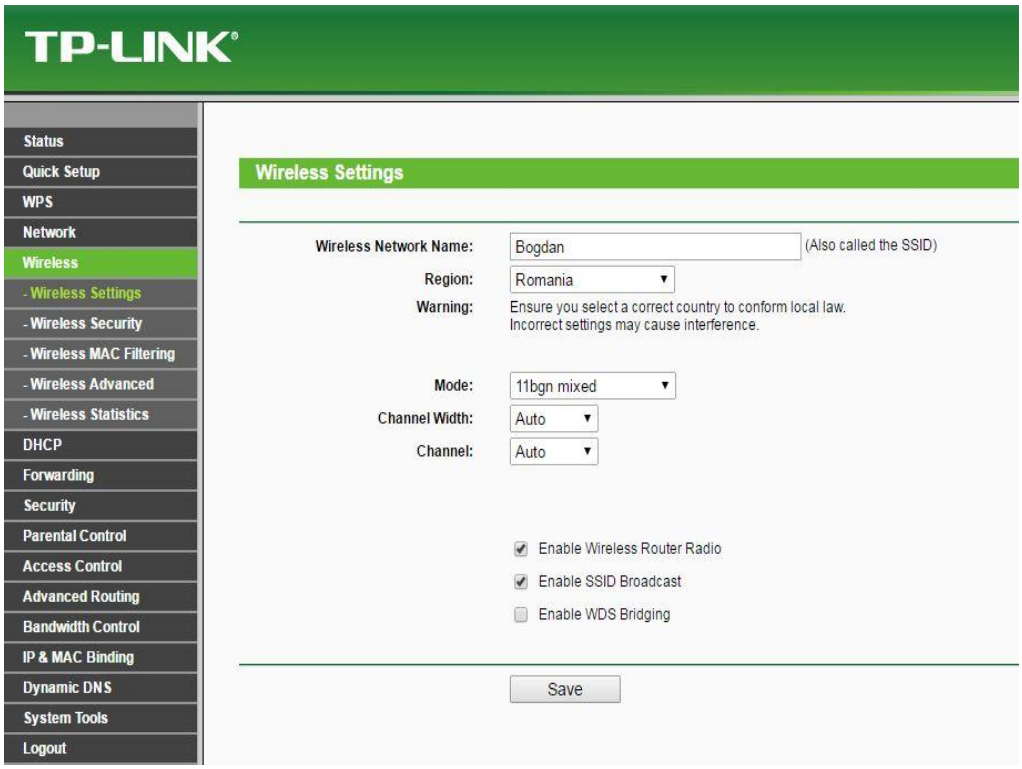

FIG. 3. Deactivating SSID Broadcast

Using Kali Linux and Pixiewps, we assessed the security of wireless networks facing a brute force attack.

With a few commands, there can be displayed the neighbour networks and some of their parameters like: channel, signal power (RSSI), the WPS version (fig.4).

Configuring the router in such a way that the network and its parameters will be invisible, the software will not detect the existence of the network (fig.5).

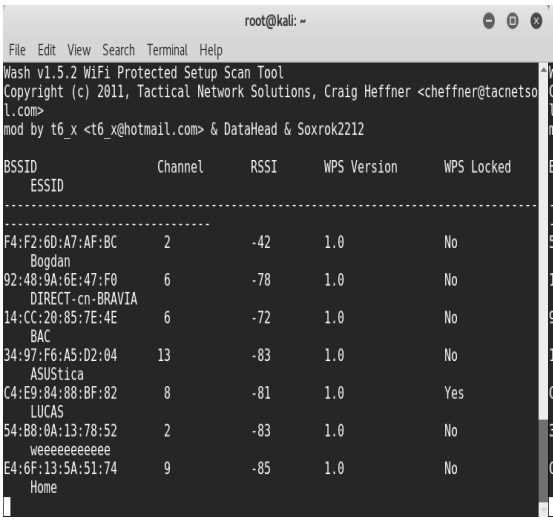

FIG. 4. "Bogdan" network visible; SSID Broadcast enabled

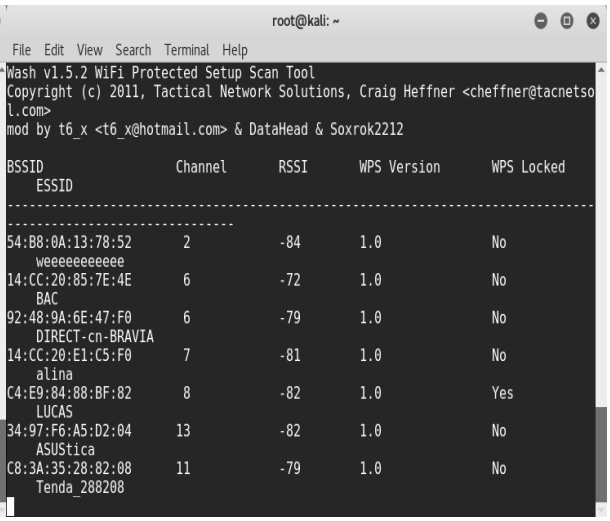

FIG. 5. "Bogdan" network hidden; SSID Broadcast deactivated

Disabling the WPS will further increase the security of the network, by closing the way an attacker could receive a valid WPA/WPA2 key.

4. CONCLUSIONS

Some practical solutions have been proposed in this paper, together with the specific test environments, appropriate operating systems and special security breach scenarios.

The Telnet protocol is recommended to be used in private networks (with lower exposure to intruders), not in public networks where attackers can take advantages of a security breach. For public networks, it can be used the SSH.

To avoid attacks based on SQL Injection, application developers and testers must conduct test scenarios for this type of security breach before the application is released.

To enhance the security of a wireless network, the router must be configured with different settings than the default ones (WPA/WPA2) and the password should be strong, at least 15 characters including small and capital letters, numbers and special characters – the strength of a longer password was demonstrated using Kali Linux. Also the highest supported security setting should be used, that is supported by all the necessary devices in the network (e.g. if all devices support WPA/WPA2 with AES, then WPA/WPA2 with TKIP should be disabled to avoid the fallback to a weaker security mode). Also the WPS should be disabled in order to maximize the security of the network.

5. REFERENCES

[1] http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html, accessed on March 19, 2017;
[2] Javvin Technologies, *Network Protocols Handbook*, Second Edition, ISBN 0-9740945-2-8, 46;
[3] http://www.differencebetween.net/technology/internet/difference-between-telnet-and-ssh/, accessed on February 7, 2017;
[4] J. Gilmore et al, *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, RFC7250, 2014;
[5] Sorin Zamfir, Titus Balan, Florin Sandu, Iulian Iliescu, *A Security Analysis on Standard IoT Protocols*, Applied and Theoretical Electricity (ICATE), 2016 International Conference;
[6] Eclipse Paho, http://www.eclipse.org/paho/, accessed on February 11, 2017;
[7] Eclipse Californium, http://www.eclipse.org/californium/, accessed on February 11, 2017;
[8] OpenSSL, https://www.openssl.org/, accessed on February 10, 2017;
[9] http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm, accessed on February 9, 2017;
[10] http://www.tp-link.ro/faq-417.html, accessed on March 10, 2017.