10.19279/TVZ.PD.2016-4-2-11

SECURITY SOLUTION FOR ATTACK VECTORS ON PORTABLE COMPUTERS DATA AND COMMUNICATION

SIGURNOSNO RJEŠENJE ZA VEKTORE NAPADA NA PODATKE I KOMUNIKACIJU PRIJENOSNIH RAČUNALA

David Pavičić[1], Roman Domović[2]

[1]Libertas International University
[2]Zagreb University of Applied Sciences

Abstract

In this paper we present a solution for an encrypted environment for portable computers in order to preserve the confidentiality of data and the security of its communication. There are at least two potential attack vectors on confidential information stored on a device. The first attack vector is achieved through an insecure network connection, while the other is physical access to an insufficiently protected device. For both attack vectors we offer protection solutions. To protect the network connection we offer an implementation of OpenVPN virtual private network driven by Raspberry Pi device from the user's home network, while for physical protection TrueCrypt is used for full disk encryption. For added security of internet traffic we are proposing the implementation of Tor anonymous encrypted connection, driven by a Raspberry Pi device as an access point (AP).

Keywords: *Security, Portable Computers, Data, Communication, Raspberry Pi*

Sažetak

U ovom radu prezentiramo rješenje za kriptirano okruženje za prijenosna računala da bi se očuvalo povjerljivost podataka i sigurnost komunikacije. Postoje bar dva vektora napada na povjerljive informacije pohranjene na uređaju. Prvi vektor je internetska veza kroz nesigurnu mrežu, a drugi je fizički pristup do nedovoljno zaštićenog uređaja. Za oba vektora napada nudimo zaštitna rješenja. Da bi se zaštitila internetska veza nudimo implementaciju OpenVPN privatne virtualne mreže pogonjene putem Raspberry Pi uređaja iz korisnikove kućne mreže, a za potpunu fizičku zaštitu tvrdoga diska koristi se TrueCrypt. Za dodatnu sigurnost internetskog prometa predlažemo implementaciju Tor anonimne kriptirane konekcije pogonjene putem Raspberry Pi uređaja kao pristupne točke.

Ključne riječi: *Sigurnost, Prijenosna računala, Podatci, Komunikacija, Raspberry Pi*

1. Introduction

1. *Uvod*

At the present time there is a growing number of users who use their private laptops and mobile devices for official purposes. We can assume that one reason is the convenience of using one device for all purposes with all data held in one place and the other reason is that more and more people can afford better equipment than they would get from the company they work for. This trend presents a major problem in keeping confidential information secure, because such user takes his equipment and leaves the security of the corporate network. He can connect to potentially unsafe and unprotected networks in cafés, restaurants, hotels, airports and so on. In those cases, communication and confidential data like business documents, financial information or any other kind of sensitive data are in danger. Unlike before, when the user presented a risk only to himself, now he exposes the whole company because of the content he has on his device. The biggest threats are from the so called Man in the

middle attacks. A malicious person provides usually free internet access but captures all the traffic that goes through his equipment. To avoid potential exposure to such attack, it is necessary to find a solution with which a secure connection to the internet is achieved. The usage of virtual private networks appears to be a practical solution, where encrypted connection between user and output server for further connection to public networks can be achieved. A large number of corporations have servers for virtual private networks (VPNs) through which employees can connect. It would not be a problem if a user used his portable computer for official purposes only, and not for private as well. Majority of corporations have introduced various restrictions on their networks. They also monitor them. As an alternative it is possible to set up and operate a private server from the home user network. Instead of using a large server, a practical and cost-effective solution is the Raspberry Pi device [1]. In addition to its small size, it is characterized by a very low power consumption. Using an open source software, the user will establish an encrypted connection between his device and the local network in his home. Disk encryption can protect hard disks from unauthorized physical access to its data. By using Tor - anonymous network and Raspberry Pi as an access point, user can anonymously access the public network via an encrypted wireless access point. We have not yet seen this combination of disk encryption and privately operated Raspberry Pi VPN/Tor AP in the joint fight for a more secure environment, especially for Bring Your Own Device (BYOD) policy. Too many people ignore the possibility that they are putting their company and themselves in danger from data theft and/or manipulation. In order to create such a secure environment, it is necessary to perform a security assessment, analyze possible threats and accordingly devise the optimum solution. In the first section we are presenting an overview of security issues. In the second section we are analyzing security threats and attack vectors. Then we are offering security solutions for each attack vector. The paper ends with a conclusion and references.

2. Security risk assessment

2. *Sigurnosna procjena rizika*

If a user carries valuable and confidential data on his portable computer and wants to share it and communicate over the internet, he is exposed to direct and indirect physical attack on his equipment and interception of his communication. This makes two attack vectors on his data. Direct physical attack on the data can be performed if an adversary gets in touch with the user's portable computer. The device may have a password set for accessing the operating system. If there is no password, an adversary can easily get to unprotected data. If there is a password, it can be bypassed by password recovery tools like John the Ripper, both on Linux and Windows, or in case of Windows by Microsoft Diagnostics and Recovery Toolset. There is also an option of removing the hard drive from the user's portable computer and accessing it on another computer where the password will be ignored. Indirect attacks are possible through some kind of Trojan horse by which adversary takes control over the computer without the host's knowledge. Interception of communication can be done through Man in the middle attacks. A user attending a conference, staying in a hotel, cafe, airport etc. is exposed to different attacks while using the provided - potentially insecure - connection to the internet. Usually he has no insight into who is operating the provided network, what security policy is in place and who could be intercepting the communication.

3. Proposed security solutions

3. *Predložena sigurnosna rješenja*

In order to provide protection from both attack vectors, we are proposing an optimal solution by combining TrueCrypt for disk encryption, OpenVPN for virtual private networking run by a Raspberry Pi device and Tor for anonymous networking powered by a Raspberry Pi device as an Tor Access Point.

3.1 Disk encryption

3.1 *Enkripcija diska*

Encryption of disc data is a method in which data is being protected from an unauthorized reading in a way that encryption algorithms turn the data into unreadable code. If a person has physical access to the device whose data is encrypted, without entering a password and/or keys he would not be able to understand the meaning of the data because it would seem to be just randomly scattered characters. This segment of protection protects the device and the data in case the device is stolen or accessed without permission. Disk encryption can be either software or hardware based. There are two main classifications with the data disk encryption approach: full disk encryption (FDE) and file/folder encryption. Full disk encryption represents the encryption of all data on the hard disk. File/folder encryption encrypts individual files or folders. In this paper we are using TrueCrypt 7.1a software for disk encryption. TrueCrypt is an open source software for so-called on-the-fly encryption (OTFE), developed by TrueCrypt Foundation in 2004. On-the-fly encryption means that the data is automatically encrypted or decrypted at the time when it is being loaded or saved into the system. The very process of encryption or decryption takes place in RAM (Random Access Memory). Although there are attacks on TrueCrypt which can be successful [2] they are not easy to perform and therefore we find TrueCrypt to be an optimal solution for easy to set up protection of hard disk data. Strong antivirus software and knowledge about the existence and functionality of various types of malware is required to defend against indirect attacks on the encrypted data.

3.2 Virtual Private Networks

3.2 *Virtualne privatne mreže*

Virtual private networks (VPN) connections are the type of point to point connections, which are established through private or public networks. When it comes to public networks, most connections are achieved through the Internet. The VPN client with the help of specific Transmission Control Protocol / Internet Protocol (TCP / IP) protocol, called tunneling protocols calls a virtual port on a VPN server. If the VPN server authenticates the client it then allows him to transfer the traffic between its local network and the client. In this paper we use OpenVPN [3]. OpenVPN is an open source software for implementing virtual private networks by author James Yonan. OpenVPN comes with a small practical Easy_RSA package to manage and generate cryptographic keys based on OpenSSL Command tool [4]. Selection of the key size itself depends on several factors. First we need to know the hardware limitations of the server - in our case the Raspberry Pi - and client, because longer key requires higher processing power. Increased operations represent a higher energy consumption. Energy consumption has a greater weight in systems where the device due to the instability of energy networks often depends on spare batteries for operations or is permanently dependent on them (e.g. mobile devices). Another important thing to know is which software supported key sizes are being used with the device. A large number of mobile devices do not yet support keys larger than 2048 bits, so this must be taken into account. Probably the most important thing is to determine the necessary level of security. To assess the importance of the secret data to be protected and find the corresponding key size. Recent attacks (for example see [5]) suggest keys 2048-4096 bits long, while american NIST (National Institute of Standards and Technology) recommends using exactly 2048 bit RSA key [6]. The Easy_RSA program provides us with a tool for the next crucial step of creating a Certification Authority. In cryptography, Certification Authority or CA is the body that issues digital certificates. In this case, instead of commercial certification authorities, we used the mentioned tool. For a client to be able to authenticate himself, it is required to generate a client key. Theoretically it is possible to generate only one key and distribute it to all customers, but with doing so only one client can be active at any given time. To protect a generated key that is currently in plain text format, it is necessary to encrypt it. Each created client key is encrypted by using the 3DES encryption. For the realization of a

secure connection OpenSSL will be used, and the keys are located in the keys directory. In order for the two computers, whether client or server, to exchange the secret keys over an insecure network a system for that exchange is required. We are using the Diffie-Hellman method. Since our Raspberry Pi VPN server will be accessible from the internet it is a good practice to try and make it a little bit more resilient to Denial of Service (DoS) attacks. DoS attacks are attacks aimed at generating a large number of inquiries to choke server services and to disrupt its normal operations. OpenVPN package includes a built-in functionality to fend-off such attacks. It will generate a static authentication code based on a hash function. If the server does not detect the generated client code, it will not accept the authentication request, let alone handle it.

3.3 Raspberry Pi as a Tor access point

3.3 *Raspberry Pi kao Tor pristupna točka*

For added security and anonymity on the net, we used Tor [7]. Tor is a free program for establishing anonymous communication through a volunteer operated network of Tor nodes. The users Tor client software downloads a list of available nodes from a directory server, from which he then randomly chooses a few to connect through. Each relay node knows only about his connection to the neighboring one, and each of the steps is encrypted with a different set of keys. To make sure that all the users devices always use the Tor network when accessing internet resources and for future ease of use we used a Raspberry Pi as an access point. It channels all its communication only via the Tor network regardless of which of our user's device connects to it. The user doesn't even have to make any changes to his device or install any software since the Tor AP will handle all the needed operations. By the early 2015, over five million Raspberry Pi devices were sold around the world and that was before the new Raspberry Pi 2 model was released [8]. All these devices come with the same default settings, which represent security risk if they are not changed. We will recommend a few steps that should be made to lower the risk - we used these changes for our Raspberry Pi VPN server as well. A policy for regular package updates should be set. Package updates except functional additions and repairs also bring out security patches which correct security vulnerabilities. Furthermore, a change to the default usernames and passwords should be done. The default username is "pi" and the password is "raspberry". Without changing the username and password, all further steps are almost worthless. Setting up a proper password is a good first step, but by changing the username we are adding one more step. If the device is under some kind of attack where the attacker tries to guess the access data, than it has to be done for both - password and username. In the realm of cracking passwords, Brute force attack is often used. Brute force attack is a cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to the problem [9]. Basically, attacker is trying to guess a password by systematically combining all possible combinations of characters. The attacker can also apply Dictionary attack which is carried out by using some large, exhaustive list of words, phrases and frequent passwords. Modern attacks on passwords combine brute force attacks, dictionary attacks and certain password patterns through the usage of cracking software like Hashcat, Hash Manager or Extreme GPU Bruteforcer in order to shorten the time of cracking. For ease of future maintenance, improvements and for eliminating the need for a separate monitor and keyboard for our Tor AP we have to have secure remote access. We used Secure Shell (SSH). SSH is a cryptographic network protocol for secure textual communication with the remote computer. SSH with its two versions SSH-1 and SSH-2 was designed as a replacement for the relatively insecure Telnet and similar application protocols for the remote access. The concept on which it is based upon is the public key cryptography concept. The user with automatically generated public/private key authenticates his computer and achieves an encrypted connection. Upon establishing a connection the user still must authenticate himself with the password. Another approach to authentication is in manual generation of both public and private key, after which

additional authentication with password is not required. Public keys are installed on computers that allow access to the computer with the corresponding private key. The private key itself is never a part of a trust establishing traffic and it is not sent through a public network. It only checks its existence. All the recent distributions of the operating system Raspbian come with pre-installed SSH package, so it is enough to set a static IP address on the device. A static address is necessary so that the device would be able to be uniquely addressed.

4. Conclusion

4. *Zaključak*

The Raspberry Pi device in the role of the VPN server and Tor access point proved to be a very good choice. In addition to its relatively low purchase price and low power consumption it provides near silent operation. In addition, it does not require an additional source of cooling, much further maintenance and even a lot of space. OpenVPN package has provided all the necessary tools for the creation of a certification authority, server and client keys, a VPN server-side and even protection against denial of service attacks. This solution provides an encrypted transmission of data between the user's device and the VPN server local network. This means that a user's request for some content from the internet is first encrypted to reach the VPN server which decrypts the message and sends it to the destination. The destination does not respond to the user but responds to the VPN server that encrypts the response and returns it to the user. The Tor project provided a way for achieving anonymity on the network. In the physical approach TrueCrypt provided the necessary tools to protect the data with full disk encryption, making the data unreadable without a secure password and/or key. Whether it is about the protection of private or official data, a small investment in time and money for the realization of such an approach in securing a portable computers data can be well worth it.

5. References

5. *Reference*

[1] Raspberry Pi. https://www.raspberrypi.org/products/; (08.02.2016.).

[2] Schneier, B.; "Evil Maid" Attacks on Encrypted Hard Drives; 23.10.2009. https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html; (06.02.2016.).

[3] OpenVPN; https://openvpn.net/; (08.02.2016.).

[4] Pellegrini A., Bertacco V.; Austin T.; Fault-Based Attack of RSA Authentication; 2010 Design, Automation and Test in Europe Conference (DATE-2010); http://web.eecs.umich.edu/~taustin/papers/DATE10-rsa.pdf; (7.2.2016.).

[5] GnuPG; Frequently Asked Questions; 11.4, 11.5; https://www.gnupg.org/faq/gnupg-aq.html#no_default_of_rsa4096; (7.2.2016.).

[6] https://www.torproject.org/. (08.02.2016.).

[7] Upton L.; Five Million Sold; http://www.raspberrypi.org/five-million-sold/; (3.5.2015.).

[8] Internet Engineering Task Force (IETS); Internet Security Glossary, Version 2; http://tools.ietf.org/html/rfc4949; (07.02.2016.).

AUTOR · *AUTHOR*

David Pavičić

David Pavičić, M.I.T. is the head of the ICT department Libertas at the Libertas International University in Zagreb. He went to Zagreb technical school where he graduated in computing. During collage years, at the Polytechnic of Zagreb where he got he's master in information technology, he's main interests focus on computer networking and information security. As the head of ICT department he's jobs include the planning and development of new IT technologies, assessing and handling threats to information security and document security, integrity and authenticity.

Roman Domović

Dr. sc. Roman Domović, prof. is a lecturer at the Zagreb University of Applied Sciences at the Department of Information Technology and Computing. He went to X. mathematical gymnasium where he graduated physics, after which he attended University of Zagreb and graduated in the field of Information sciences and Phonetics. At the same university he earned his doctoral degree in the field Information and Communication sciences. His research interests are applied cryptography, classical cryptography and information warfare. He is an author of several scientific articles in the field of Information and Communication sciences.