



FACULTY OF INFORMATION TECHNOLOGY  
UNIVERSITY OF VITEZ

ТАМБОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ Г. Р. ДЕРЖАВИНА Г. ТАМБОВ



INTERNATIONAL JOURNAL

ZBORNIK RADOVA ISSN 1986-5694

# INTERNATIONAL JOURNAL

## of Information and Communication Technologies

Scientific journal of theory and practice in business informatics and information-communication technologies

3.



*ISSN 1986-5694*

*Scientific journal of theory and practice in business informatics and information-communication technologies*

*Number 3.*

**INTERNATIONAL JOURNAL  
OF INFORMATION AND COMMUNICATION TECHNOLOGIES  
FACULTY OF INFORMATION TECHNOLOGY, UNIVERSITY OF VITEZ  
and  
TAMBOV STATE UNIVERSITY NAMED AFTER G.R. DERZHAVIN**

February 2015.

## **PUBLISHERS:**

*UNIVERSITY "VITEZ" VITEZ, Bosnia and Herzegovina and  
TAMBOV STATE UNIVERSITY named after G.R. Derzhavin, Russia*

## **EDITORIAL**

*Prof. Mirko Puljic PhD, Rector, University „Vitez“, Prof. Lazo Roljic PhD, Dean FIT University „Vitez“, Asst. Prof. Hadzib Salkic PhD, Asst. Dean for academic affairs FIT University „Vitez“, Mr.sci Senad Tatarevic, coordinator for international cooperation University „Vitez“, Mr.sci Darijan Soldo, senior asst. FIT University "Vitez", Mr.sci Mahir Zajmovic, senior Asst. FIT University „Vitez“, Nermina Konjalic, FIT, Univerisity „Vitez“,*

*Юрьев В.М., д.э.н., профессор, ректор ТГУ имени Г.Р. Державина, Пахомов М.А., д.э.н., профессор, зав. кафедрой бизнес-информатики ТГУ имени Г.Р. Державина, Мукин С.В., к.т.н., профессор кафедры бизнес-информатики ТГУ имени Г.Р. Державина i Старцев М.В., к.п.н., доцент кафедры бизнес-информатики ТГУ имени Г.Р. Державина*

## **EDITOR IN CHIEF**

*Assistant prof. Hadzib Salkic, PhD*

## **DESIGN AND PREPRESS**

*Almira Salkic, BA*

## **ADDRESS OF PUBLISHER**

*Ulica Skolska 23  
72270 Travnik  
Bosnia and Herzegovina*

*ISSN 1986-5694*

*Number 3.*

## **CONTACT**

*journal\_fit@fit.co.ba  
+387 30 519 750  
+387 30 519 759*

**WEB PRESENTATION AND E-COMMERCE  
AT THE EXAMPLE OF PUBLIC INSTITUTION 'RETIREMENT HOME WITH  
DISPENSARY'**

Ana Marić<sup>1</sup>, Hadžib Salkić<sup>2</sup>, Almira Salkić<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

ana.maric@unvi.edu.ba, hadzib.salkic@unvi.edu.ba, almira.salkic@unvi.edu.ba

..... 7

**CREATING OF EFFECTIVE WEB SITE**

Marko Stergulg<sup>1</sup>, Bajro Ljubunčić<sup>2</sup>, Admir Škaljić<sup>3</sup> and Džemal Vejsil<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

marko.stergulg@unvi.edu.ba, bajro.ljubuncic@unvi.edu.ba, admir.skaljic@unvi.edu.ba,  
dzemal.vejsil@unvi.edu.ba

..... 16

**SECURITY OF INFORMATION**

**EMAIL SECURITY**

Hadžib Salkić<sup>1</sup>, Almira Salkić<sup>2</sup>, Amra Mirojević<sup>3</sup>, Dajana Marić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

hadzib.salkic@unvi.edu.ba, almira.salkic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba,  
dajana.maric@unvi.edu.ba,

..... 26

**WIRELESS WI-FI COMPUTER NETWORK**

**AND**

**SECURITY WI-FI NETWORK**

Mahir Zajmović<sup>1</sup>, Arminka Šabanović<sup>2</sup>, Sidika Šabić<sup>3</sup>, Damir Pivić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

mahir.zajmovic@unvi.edu.ba, arminka.sabanovic@hotmail.com, sidika.sabic@gmail.com,  
damir.pivic@yahoo.com

..... 35

**USE OF THE PROTECTED WEB NETWORK – SSL PROTOCOL**

Mahir Zajmović<sup>1</sup>, Alma Bešić<sup>2</sup>, Adrijana Veselinović-Dolić<sup>3</sup> i Nermina Konjalić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

mahir.zajmovic@unvi.edu.ba, alma.besic@gmail.com, adrijana.veselinovic@gmail.com,  
nermina.konjalic@unvi.edu.ba

..... 43



## **ESSAY ON INFORMATION SAFETY**

Amela Begović<sup>1</sup>, Hadžib Salkić<sup>2</sup>, Amra Mirojević<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

amela.begovic@gmail.com, hadzib.salkic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba

50

## **DATA PROTECTION USB MEMORY STICK USING THE TRUECRYPT PROGRAM**

Hadžib Salkić<sup>1</sup>, Adin Lemo<sup>2</sup>, Amela Haračić<sup>3</sup> i Fatima Husejnović<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

hadzib.salkic@unvi.edu.ba, adin.lemo@gmail.com, amela.haracic@gmail.com,  
fatima.husejnovic@gmail.com

56

## **SALES OF PHOTOGRAPHS**

Bajro Ljubunčić<sup>1</sup>, Amra Mirojević<sup>2</sup>, Almira Salkić<sup>3</sup> and Emir Brčanić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

Bajro.ljubuncic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba, almira.salkic@unvi.edu.ba,  
emir.brcaninovic@unvi.edu.ba

63

## **BUSINESS INTELLIGENCE**

Grabus Elvis

UNIVERSITY OF "VITEZ" VITEZ

elvis.grabus@unvi.edu.ba

71

## **DATA ENCRYPTION**

Benjamin Destanović<sup>1</sup>, Senida Kakeš<sup>2</sup>, Hasmir Musić<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

benjamin.destanovic@unvi.edu.ba, senida.kakes@unvi.edu.ba, hasmir.music@unvi.edu.ba

38

## **IDENTIFYING TYPES OF ATTACK**

Alen Osmanagić<sup>1</sup>, Senida Kakeš<sup>2</sup>, Benjamin Destanović<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

alen.osmanagic@unvi.edu.ba, senida.kakes@unvi.edu.ba, benjamin.destanovic@unvi.edu.ba

88

## **APPLICATION OF IT AND IT TOOLS IN MEDICINE, MYCIN**

Sead Hamzić

Kladanj

sead.hamzic@unvi.edu.ba

99

## **INTRODUCTION BY THE EDITOR**

---

*Asst. Prof. Hadzib Salkic, PhD*

*Dear readers,*

*Please find the third edition of International Journal of information and communication technologies.*

*In this number, you can read different contents of scientific works and research papers from several areas of ICT. Topic of this issue is related to field of E-commerce, data protection and business intelligence. This is first issue on English language only and with changed name from Proceedings into International Journal of information and communication technologies.*

*The following issue of International Journal should be expected in March or April next year having the following topic such as „The ICT area in teaching process“ which should be name of the second International conference organised by FIT-, University „Vitez“.*

*With respect and hope that we will continue to cooperate, please receive the warmest regards.*

## **INTRODUCTION BY THE DEAN OF FACULTY OF INFORMATION TECHNOLOGY UNIVERSITY VITEZ**

---

*Prof.dr Lazo Roljić*

*Dear readers,*

*In front of you is the third edition of International Journal of information and communication technologies issued by Faculty of information Technology University of Vitez, journal for theory and practice in the field of business informatics and information – communication technologies. Journal is our effort to, all those who follow or are interested in this dynamic area, provide an opportunity to find out what is new in the area and what our experts and scholars are doing in this field, and to provide an opportunity for everyone to write about it and contribute accordingly. By publishing this Journal, we intent to bring, scientific and technical achievements in the field of IT, computer engineering and, overall, information – communication technologies and their application in several different fields of life and work to students of first, second and third cycle of studies according to Bologna Declaration as well as to assistants and professors of our University. Idea behind is to present our University to wider audience and public. At the same time, we wish that the regular publishing of this Journal becomes a scientific challenge to all whom it is intended so they participate in the publication of their work and together with us enjoy in it. Journal is edited according to the criteria of scientific and professional journals and is in accordance with the Book of rules of the University publishing activities. Scientific papers are reviewed and, as such, will be referenced.*

**WEB PRESENTATION AND E-COMMERCE  
AT THE EXAMPLE OF PUBLIC INSTITUTION 'RETIREMENT HOME WITH  
DISPENSARY'**

Ana Marić<sup>1</sup>, Hadžib Salkić<sup>2</sup>, Almira Salkić<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

ana.maric@unvi.edu.ba, hadzib.salkic@unvi.edu.ba, almira.salkic@unvi.edu.ba

***1. INTRODUCTION***

Retirement home (BiH, penzionerski dom) is an institution with main task to provide nursing and medical care, good nutrition, work activities and everything that makes life complete to elderly people in accordance to their age. With good care they can live quality and dignified life. Popularity of retirement homes exceeds the higher level in Bosnia and Herzegovina. Retirement homes also follow European trends of growth. Every fifth inhabitant of Bosnia and Herzegovina is older than 65 so retirement home projects are becoming more popular and profitable business.

**Photo No1:** "Retirement home with dispensary"



**Source:** Archive of "Retirement home with dispensary"

To provide better promotion this type of institutions, especially at the era of Internet society, significant investments are related to promotions via Internet. This involves e-marketing, web presentations, as well as the possibility of using e-commerce services. Their usage will be presented at the example of retirement home called Public institution "*Retirement home with dispensary*".

## **2. E - MARKETING AND WEB PRESENTATION**

Marketing is around us in one form or another, but the methods of marketing have changed and improved and they are connected to modern communication technologies nowadays. Electronic marketing (e-marketing) refers to the application of marketing principles via electronic media, especially Internet. Main task of e-marketing is to provide information's about retirement home to targeted audience, and to make better connection between retirement home and users. For best e-marketing we need to make good marketing plan which defines:

- Who are the users of services?
- What is the vision of retirement home?
- What are the advantages of retirement home in relation to market competition?

**PhotoNo2: E-marketing**



**Source:** [www.axisgmo.com](http://www.axisgmo.com)

Key advantage in use of e-marketing compared to conventional marketing is the lower price. Other benefits of e-marketing are: target audience - right consumer, e-marketing enables us to take advantage of the growing importance of social media, we can make purchases 24/7, increased interactivity, increased ability to track results.

Good design of web presentation leaves a positive impression to our audience. The web offers many solutions for delivering information to audience which includes Flash, PDF, video, photo, slideshow. A web presentation offers a high level of interaction and responsiveness that a desktop presentation can't provide.



## 2.1. Creating web presentation with Joomla 3.X

Joomla is Content Management System (CMS) which enables simple editing and control of the content of our website. Joomla is easy to use and if you are able to surf the Web, interact with interfaces and forms, handle computer tasks, you are able to use Joomla.

**Photo No3:** Joomla around the world



**Source:** [www.global-visiontech.com](http://www.global-visiontech.com)

### 2.1.1. Requirements for Joomla

When creating our web site, first of all is to get a domain name, which is our private address on the Web. Domain name is human readable Internet address of website. You have to, for an example for retirement home with name 'Retirement home with dispensary' domain name is **www.penzionerskidom.ba**. Next step is to find a web hosting service. For this domain name, we use **Avalon Premium Hosting**. Our next step is to design, build and upload our website.

**Photo No4:** Avalon Premium Hosting



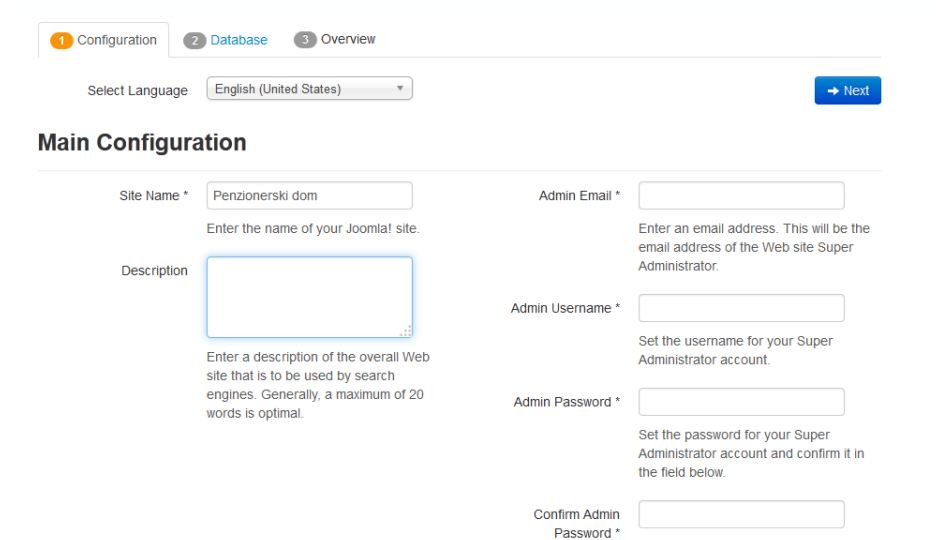
**Source:** Own source

With Joomla you can design themes and templates for your website, but you can also use already made themes and templates for free. There are also extensions that you can download for your website. There are some recommended extensions for website: News display, Multimedia display, Banner, Contact forms, Forum.

## Installing Joomla

We need to complete two tasks before we can install Joomla on server. The first one is installing Joomla 3.x package files and second, to make database for Joomla use. When we finish download Joomla installation package we have to move the package to server. I use FileZilla FTP Client for moving files to server. Next step is to open browser and type [www.penzionerskidom.ba](http://www.penzionerskidom.ba) to start installation process.

**Photo No5:** Installing Joomla! for domain penzionerskidom.ba



The screenshot shows the Joomla! installation Configuration step. At the top, there are three tabs: '1 Configuration' (active), '2 Database', and '3 Overview'. Below the tabs, there is a 'Select Language' dropdown menu set to 'English (United States)' and a blue 'Next' button. The main section is titled 'Main Configuration' and contains several input fields with labels and instructions:

- Site Name \***: Input field containing 'Penzionerski dom'. Below it, the instruction reads: 'Enter the name of your Joomla! site.'
- Description**: A large text area. Below it, the instruction reads: 'Enter a description of the overall Web site that is to be used by search engines. Generally, a maximum of 20 words is optimal.'
- Admin Email \***: Input field. Below it, the instruction reads: 'Enter an email address. This will be the email address of the Web site Super Administrator.'
- Admin Username \***: Input field. Below it, the instruction reads: 'Set the username for your Super Administrator account.'
- Admin Password \***: Input field. Below it, the instruction reads: 'Set the password for your Super Administrator account and confirm it in the field below.'
- Confirm Admin Password \***: Input field.

**Source:** Own source

We need to fill information shown on the photo above:

- **Site name:** The name of you website, in this case – Retirement home.
- **Description:** Enter the description of your website. You are able to change Site Name and Description later on Site Global Configuration.
- **Admin Email Addresses:** Enter a valid admin email address.
- **Admin Username:** Joomla uses a default 'admin' as the username for Super User. You can leave it as it is. You can change it in the Administration interface later.
- **Admin Password:** Try to use a difficult password.
- **Site Offline:** You can click Yes or No box and this means installation is complete. You can use Site Global Configuration in the Administration interface to change it at any time.

When everything is completed, click next button to proceed to Database Configuration. You will need to enter information about the database you will use for Joomla. After filling Database Configuration fields it is time to finalize installation. If you are new to Joomla it would be good to install sample data. If everything is ok, you will see the install at the top of the page.

**Photo No6:** Joomla! Is installed



**Source:** Own source

## 2.2. Our web site

Website www.penzionerskidom.ba is created with Joomla. Process was fun and simple with very professional results. Joomla has many benefits over the other open source management systems and this is what is making Joomla more and more popular every day.

**Photo No7:** www.penzionerskidom.ba website created with Joomla!



**Source:** Own source

**Photo No8:** www.penzionerskidom.ba website created with Joomla!



**Source:** Own source

### 3. E-COMMERCE

E-commerce is a term for any type of business that involves transfer of information across the Internet. E-commerce allows consumers to electronically exchange services and goods. There are no barriers of distance and time in this form of exchange.

**Photo No9:** E-commerce



**Source:** www.almatecsrl.com

We use e-commerce in our retirement home. We sell all kind of goods that our users make. They make postcards, clothes, souvenirs etc.

In our Joomla website we use JoomShopping extension for our online shop.

**Photo No10:** JoomShopping extension for Joomla!



The screenshot shows the JoomlaShopping extension page on Joomla.org. It features a header with the extension name, a 'POPULAR' badge, and a 'CMS' logo. Below this is a table with details: Version 4.5.0 (last update on Jun 4, 2014), Rating 4.58 out of 5.00 from 24 users, Compatibility with Joomla 2.5 and Joomla 3.x, License GPLv2 or later, Type Free Download, and Date Added 9 July 2008. At the bottom, it lists the Developer as MAXXmarketing GmbH and provides links for Download, Demo, Support, and Documentation.

JoomShopping		POPULAR	CMS	
	Version	4.5.0 (last update on Jun 4, 2014)	Rating	4.58 out of 5.00 from 24 users
	Compatibility	 	Reviews	122
	License	GPLv2 or later	Type	Free Download
	Date Added	9 July 2008		

Developer: [MAXXmarketing GmbH](#)

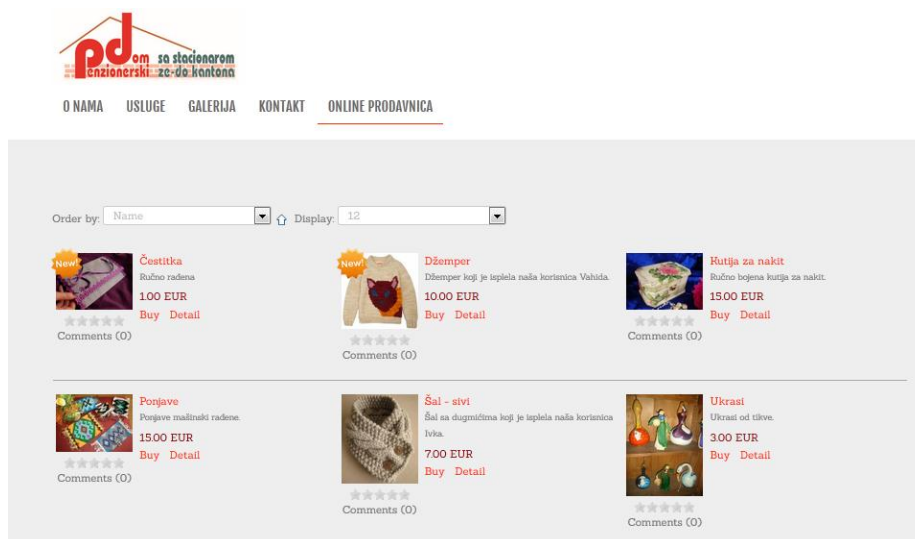
Website: [Website](#)

[Download](#) [Demo](#) [Support](#) [Documentation](#)

**Source:** extensions.joomla.org







JoomShopping extension can be used for selling different products. Products can be shown with pictures, text and audio and video files. It is very easy to use for sellers and buyers.

**Photo No11:** www.penzionerskidom.ba online shop



The screenshot shows the homepage of the www.penzionerskidom.ba online shop. The header features the shop's logo and navigation links: O NAMA, USLUGE, GALERIJA, KONTAKT, and ONLINE PRODAVNICA. Below the header is a product grid displaying six items: Čestitka (100 EUR), Džemper (1000 EUR), Kutija za nakit (1500 EUR), Ponjave (1500 EUR), Šal - sivi (700 EUR), and Ukrasi (300 EUR). Each product listing includes a thumbnail image, a 'New' badge, the product name, a brief description, the price, and links to 'Buy' and 'Detail'.

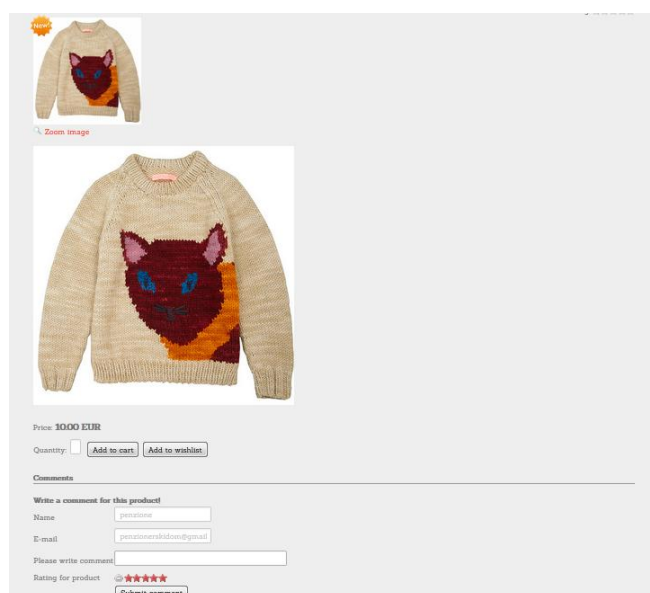
Order by:  Display:

 <b>Čestitka</b> Ručno radena 100 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)	 <b>Džemper</b> Džemper koji je isplela naša korisnica Vahida. 1000 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)	 <b>Kutija za nakit</b> Ručno bojena kutija za nakit. 1500 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)
 <b>Ponjave</b> Ponjave malinasti radene. 1500 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)	 <b>Šal - sivi</b> Šal sa dugmčićima koji je isplela naša korisnica Ivka. 700 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)	 <b>Ukrasi</b> Ukrasi od tilave. 300 EUR <a href="#">Buy</a> <a href="#">Detail</a> Comments (0)

**Source:** Own source

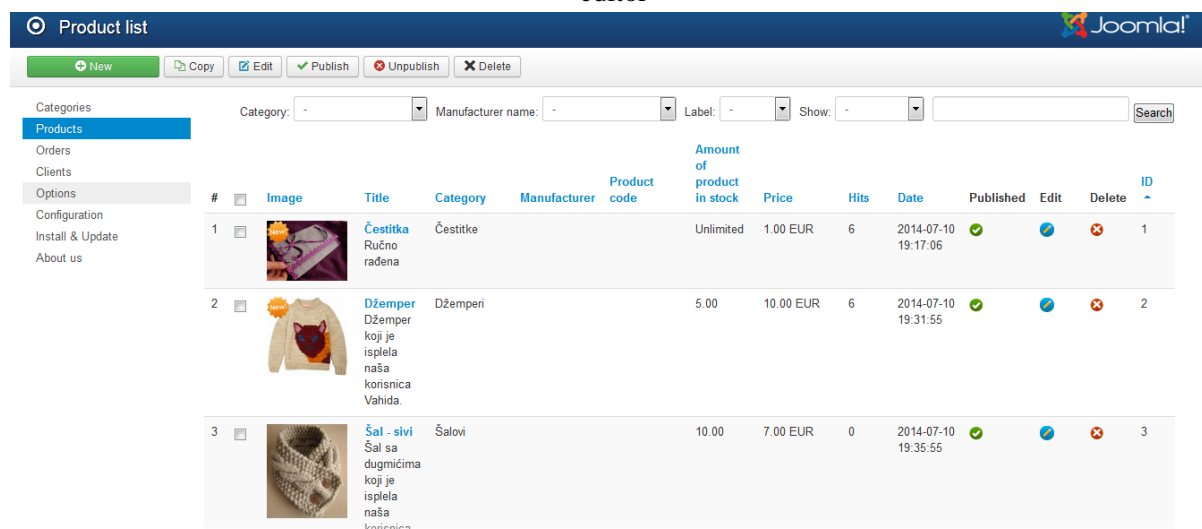


**Photo No11:** www.penzionerskidom.ba online shop



**Source:** Own source

**Photo No12:** www.penzionerskidom.ba Joomla editor



**Source:** Own source

#### 4. CONCLUSION

Joomla is Content Management System (CMS) which enables simple editing and control of the content of our website. Joomla is easy to use and if you are able to surf the Web, interact with interfaces and forms, handle computer tasks, you are able to use Joomla.

When creating our web site, first of all is to get a domain name, which is our private address on the Web. Domain name is human readable Internet address of website. You have to, for an example for retirement home with name 'Retirement home with dispensary' domain name is **www.penzionerskidom.ba**. Next step is to find a web hosting service. For this domain name, we use **Avalon Premium Hosting**. Our next step is to design, build and upload our website.

## **5. REFERENCES**

- [1] H .Lee, J., Woodrow W., M.: *Nursing and retirement home administration*, Iowa State University Press, 1966.
- [2] Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academies Press; 2001.
- [3] Sensmeier, J., and C. Delaney. "Nursing Informatics Collaboration Task Force Letter" 2004. Available at [http://www.nitrd.gov/pitac/reports/20040401\\_amia\\_himss.pdf](http://www.nitrd.gov/pitac/reports/20040401_amia_himss.pdf)
- [5] <http://www.calpers.ca.gov/> (15.07.2014.)
- [6] <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2533117/> (15.07.2014.)

## **CREATING OF EFFECTIVE WEB SITE**

Marko Stergulec<sup>1</sup>, Bajro Ljubunčić<sup>2</sup>, Admir Škaljić<sup>3</sup> and Džemal Vejsil<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

marko.stergulec@unvi.edu.ba, bajro.ljubuncic@unvi.edu.ba, admir.skaljic@unvi.edu.ba,  
dzemal.vejsil@unvi.edu.ba

### ***1 INTRODUCTION – WHY THE WEB PREZENTATION?***

The web site is the best and cheapest option for the presentation of any company or trade. It is nothing more than a document that has text, image or video material which presents a service or product to potential customers.

The increasing influence of the virtual world today is present in the real world, which has resulted in more and more things we perform with the Internet. Today we have virtual offices; we buy and entertain over the Internet. Selling from door to door is a thing of past. Web presentation today takes a major role in the interaction between buyer and seller. Today we buy so that in our favorite search browser we type the name of product or service that we want to consume in a couple of seconds we are served a full range of required products and with inspection into the price, quality, reviews and opinions of other consumers.

Access to information today is fast and widely present. The consumer wants to have as much information about the product or service for which it is interested. Seriously designed and implemented, beautiful web presentation greatly contributes to competitive advantage. For them, the visitor feels comfortably and that it "[pushes](#)" to continue his research on the product/service that we offer him.

We said that a good presentation helps achieve a better competitive advantage. Likewise, poor presentation has the opposite effect and very easily it can happen that a potential customer abandons the site. Knowing that it cannot be our goal, in this paper, we introduce our readers on what you should look out for when developing an effective web presentation.

In this paper, we try to process through several chapters the rules that must be followed when developing Web pages, theme, color choice, making the logo of pages through practical examples of implementation of the company's website where we want to create a website.

### ***2 THE RULES OF WEB DESIGN AND GUIDELINES FOR WEB PRESENTATION***

Each page of a company should be a bridge between the company as a reseller of its products and visitors as consumers of these products. Web presentation IS tool of marketing and visitor must immediately after opening page to find out what is theme of the website and what it does. If a visitor within five to seven seconds does not understand what it was about, he leaves the site.

From web presentation we must not make the book. Visitors must get as much information in as little written text. If this is not respected, it is likely that he will remain at the site. If this is not possible, it is

necessary to publish only the headlines with a short introduction text on the front and a link that leads to another page detailing informs the user about any topic.

When selecting fonts must be sure to avoid exotic, unusual and strange fonts, and is based on the use of standard fonts such as Arial and Verdana. The above fonts are legible and easy.

Registration is extremely undesirable. If necessary, it is good to take advantage of various Facebook, Google and other API functions that enable us to registered users through their existing accounts. Thus, we release our visitor completing strenuous forms, and at the same time and get all the information that may be relevant to our business.

Flash also can be irritating, especially on slow connections to the Internet. New technologies such as HTML5, CSS3, Canvas and WebKit, all effects can be replaced by other, much enjoyable to a visitor of page. With the advent of mobile internet and smart phones, Flash is becoming less popular and desirable technology.

A very important thing about web design is that the site must be optimized for all of the visitors who come from Europe and America with a very fast broadband internet access, to people who are still "struggling" with the dial-up connection (often case in Romania and Bulgaria).

We need to avoid music or video on a web page that user cannot turn off. If the topic is not possible to eject this kind of content, it is desirable to offer the user the option "Play".

Contact information's and other ways that we want to interact with the user must be visible and conspicuous. It is desirable that the web presentation enrich the existence of forums where users will be able to leave some of their comments, ideas, and suggestions. It is important that the competition and the wicked often abused forums for the purpose of causing unjustified bad reputation. If the forum is the only choice, always should carry out continuous monitoring.

What we especially have to watch out for is that the content of the web presentation has no grammatical and spelling mistakes. This is something that the user in the beginning does not inspire confidence.

In addition to the above, there are several rules which should be observed when developing websites:

1. Using input - intro page is not in vogue. Each page must be the most valuable content immediately pointed out, without having to waste time visitor clicking on "Entry" and the like.
2. No unnecessary advertisements - with every advertisement we lose visitors. After all, not even a decent serving people something that is not of their interest.
3. Easy and clear navigation is a key to the success of any good web presentation. If visitors do not know how to handle the complicated menus, it is possible that they will leave the site. That is not the point, is not it?
4. Search engine - if the site has more than one hundred documents you need to put it in a visible place a search engine that will help the visitor as soon as possible and as simple as possible obtain the desired information.
5. Visitors we should not confuse while reading lots of useless links.
6. Avoid auto interpretation of audio material - it can be sometimes very frustrating.

## **2.1    *Logotype***

The logo is the visual identity of the company. It has a very important role in each company, including the preparation of each web presentation. The importance of a logo identity as one of the reasons we have this theme into a separate subheading. The appearance of the logo is of paramount importance. Approach to designing logotype must not be superficial and amateurish. The logo should be designed in a way that the visitor website point to it which the company does, but in the way the logo is simple, understandable and recognizable. A successful logo is not one that has a lot of detail on it and decorated with various elements. Take for example the logos of world famous brands such as Apple, IBM, Microsoft, and Nike. None of them is complicated, and these are some of the most famous brands in the world. For the logo is desirable to combine multiple colors, but no more than four colors to make the logo unique. The best examples of the "colorful" logotype can be found at the company Google or eBay.

To create a quality logotype takes a lot of imagination used for creating distinctive logo in a multitude of others.

## **2.2    *Choosing colors***

With a selection of logos, the most important thing in each page's color choice.

"Color is a sensory experience that occurs when light characteristic evoke spectrum of receptors in the retina of the eye. The color can also be attributed to the surfaces of objects, materials, and light sources. It depends on their properties of absorption, reflection, or emission of the light spectrum. "

By choosing color, we give meaning to our website. For example:

- Blue is the color of the corporation (e.g. Microsoft, IBM ... at their pages dominates blue color) and reliability;
- The red color symbolizes danger, urgency, loss, alarm;
- Yellow indicates a warning, importance;
- Green - safety and profit etc.

The ideal combination for the body of the article is white or a light color and black text. With this we achieve the best contrast.

In selecting colors should not be exaggerated. These pages will look unserious for users. The site must be made with taste and should be pleasant to the eye. The number of colors used on the site must be limited to a maximum of four colors, as well as in the design of the logo.

For a good site is very important to choose a good color combination. On the Internet there are many pages that help us in selecting color combinations. Closest to us is the most famous Color Combos <http://www.colorcombos.com>.



## **2.3    *Design***

When creating a web presentation is necessary to strive towards simplicity. A large number of details are generally counterproductive because it may be that such a design overshadows the product itself or the service we provide on the site. In addition, it is very difficult sites with lots of elements and details optimize to work the same on all popular web browsers.

We are now facing with the need to adjust our sites and smart devices, making web design becomes demanding. Attention should be given to the title(s). Titles must be quite large and noticeable, color contrast must be expressed, and the color choice speaks on topics we present. Design must be simple. Only this will draw attention of visitors and make a product that we offer a central object of presentation - that is the most important.

From tasteless design better is presentation that has no design.

## **3    *TECHNOLOGY SELECTION***

When we approach to the development of the site, we want to apply the technology that is modern and in accordance with time. With the technology we need to know one rule - The more modern technology is, it is also more complex, the more it takes time to learn, but implementation is faster.

The foregoing is the reason why we have chosen HTML5, CSS3, jQuery and WebKit in making an effective website. It is very important to know all of them, so we will separately explain it.

### **3.1    *HTML5***

HTML 5 is still in the development stage, which means that on this standard and further discussed in the HTML Working Group and WHATWG mailing lists. HTML 5 (sometimes called Web Applications 1.0) is a technology developed by the WHATWG (Web Hypertext Application Technology Working Group), a group that was formed by the merger of three major producers' browser: Mozilla, Opera and Apples Safari. Behind standards stands consortium W3C (World Wide Web Consortium), the main holders of the development is Google, Apple and Mozilla. Microsoft has joined later.

It will take time until the final introduction of the new standard for creating Web pages, HTML 5 impact on the development of the Internet is strong. YouTube is already available in HTML 5 format. His example was followed by a growing number of websites especially those which provide users implementation of video content. Companies such as Google, Apple and Microsoft have started to provide support for HTML 5 in its classic and mobile browsers. It is expected that in the next few years finally define the standard for creating Web pages, and methods for their views by the user.

### **3.1.1 New elements**

Below are displayed fields for entering information into forms.

Inside the HTML5 standard is added several functional elements listed in the following list:

- input type = datetime - input the date and time in the global form
- input type = datetime-local - input the date and time in the local the global form
- input type = date - input date input
- input type = month - input month the month
- input type = time - time input
- input type = week - input the year and week
- input type = number - controlled input only numeric values
- input type = range - input numeric fields
- input type = email - controlled input email address
- input type = url - controlled input URL
- input type = search - controlled entry for local search system
- input type = tel - controlled input phone number
- input type = color - color selection through the "color wheel"
- Keygen - data entry certificate.

### **3.1.2 Content elements**

Except functioning in HTML5 are introduced and content marks that replace the div and span structures, and describe the content of the block:

- article – article
- aside - the side content
- Cite – citation
- figcaption - the title of the graphic
- Figures - graphical display
- footer - the bottom of the document
- header - the head of the document
- hgroup - leading part of the content
- NAV – navigation
- Section - part of the content.

### **3.1.3 Elements related to audio and video content**

Considering the fact that the audio and video contents become an integral part of the HTML pages, for them are introduced special tags to make it easier to include in an HTML document:

- embed - inclusion of additional plug-in
- audio - audio stream
- source - the source of audio and video content
- track - a position audio and video content

- video - video content.

### 3.2 *Cascading Style Sheets (CSS)*

Cascading Style Sheets (CSS) is a style language, which is used to describe the presentation of the document written using HTML code. As the web has evolved, were originally thrown into HTML elements to define the presentation (e.g. <font> tag etc.). Very quickly identified need for stylistic language that would relieve the need of displaying HTML content (which is primary purpose of HTML) and its shape (which is now used in CSS).

In other words, the style defines how to display HTML elements. CSS regulates the appearance and arrangement of the page.

CSS can be written within the HTML page, in three ways:

- The styles in the header of the HTML document (i.e. between <style> and / <style> element)
- Within the HTML tags, for example. <p style = "color: red"> Some text </ p>
- It can be defined in a separate document, using the call:  
`<link rel = "stylesheet" href = "some.css" type = "text / css" />`

### 3.3 *jQuery*

jQuery is one of the most popular JavaScript libraries, which in the short term become very popular because of its easy use and small resources taking on the computer.

It is used by giants like Nokia and Google, advanced programmers, but also and beginners in JavaScript. It is widely used even website designers which do not know the JavaScript, because it is very easy to learn the basic things, and for all the more complicated it is possible to find a quality plug-in.

## 4 *CREATING A WEB SITE*

### 4.1 *Planning*

Once we have chosen colors that we use, logo and technology that we intend to use, the next step is to sketch the site. The sketch sites can do on paper or in a software tool like Wireframe Sketcher Studio.

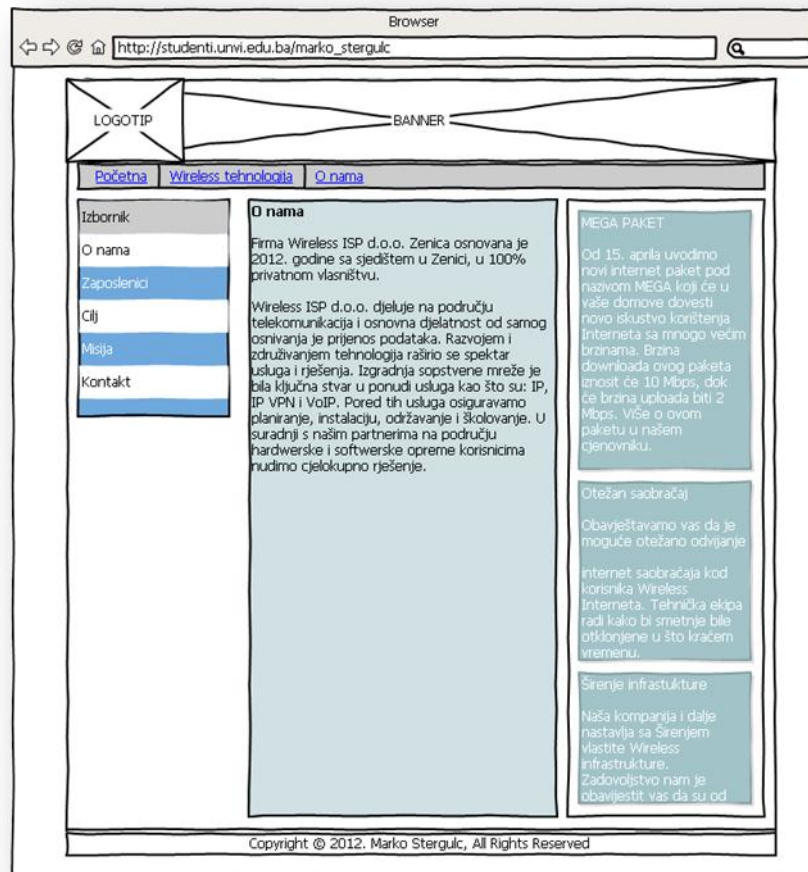
We must pay attention, as we outlined in the previous section of this paper, is the simplicity of the web presentation. Web presentation does not contain unnecessary elements that will catch the attention of visitors from that important content.

The content that is considered essential must occupy a central part of the site.

The presentation can have horizontal and vertical menu. At this site, we decided to use one vertical menu on the left side the website and only one horizontal menu at the top of the page. In addition, the

site may contain a horizontal menu at the bottom of the page. Because of reducing the number of elements, we decided not to add that extra menu.

Vertical left menu is conceptually refers to the firm. There is where visitor meets with the goals, mission and company in general, while the horizontal menu relates to the offer and price list.



*Picture 1 Sketch of website for the company Wireless ISP*

Top of the page is reserved for the banner and logo of the company. Company logo with banner indicates that this is a company that provides Internet access services over wireless infrastructure. This has the rule that a user within 5 to 7 seconds should know what the theme of the page is.

The right part of website is important because this shows all the important news that users informed about the news and the potential problems that the company faces. Because of its importance, it should be emphasized. Implementation of it is in changing the color of the background and red box around it (red means danger - alarm, as mentioned in one of the previous chapter). Within this framework, the left side should present news that will alert the user about an issue

When selecting the colors on the page I kept the rule that should not be used more than four up to five colors including: blue, gray, black, white and a red for frame.

## 4.2 Creating the structure

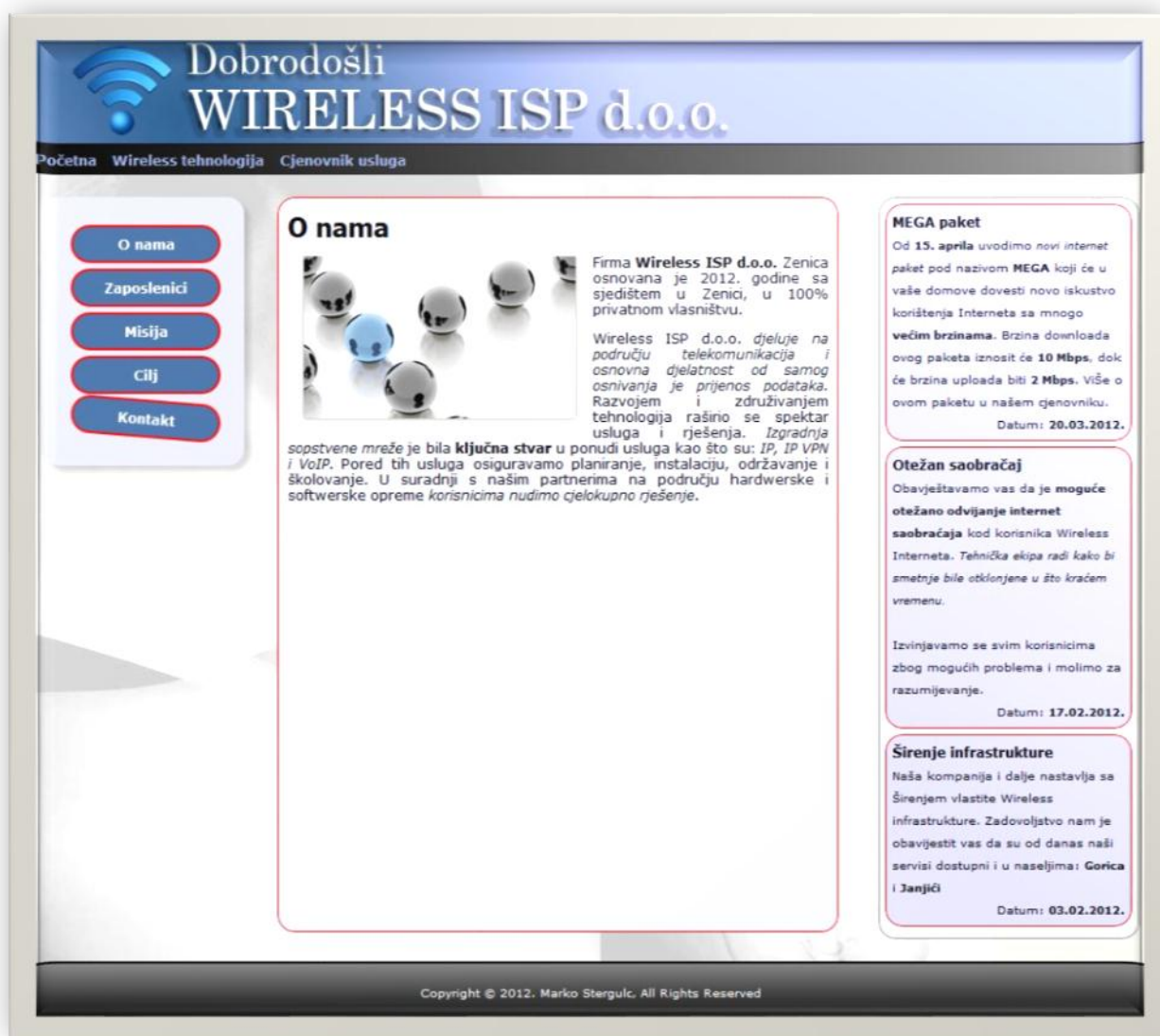
HTML5 has introduced a range of new features such as: `<header>`, `<footer>`, `<nav>`, `<article>`, `<section>` and `<time>`. Using the newly introduced elements of a website becomes a semantic clearer. For example, if you navigate websites put inside the designated `<nav>` element - our viewer that can recognize and thereby facilitate movement of the website visually impaired and blind people. In addition semantically clearer website contributes to optimizing content for search browsers (SEO). However, if we do not use a modern web browser that has support for HTML5, there may be problems with the display of the new HTML5 elements.



*Picture 2 The structure of the HTML 5 websites*

After we finished with the development of the structure of our HTML5 website, we start with the styling of our site. We do this through CSS.





Picture 3 The final page layout of the company Wireless ISP d.o.o.

## 5 CONCLUSION

During of ours professional career in various companies repeatedly changed page design of these firms. Clients were most unhappy if the design was complicated, with lots of elements and colors. An additional problem in these pages was that it was those very often, especially on very old computers such as our market is still a reality, opening very slowly.

This approach of creating web presentations knows "chase" visitors, and we need to afraid when design them. The purpose of this papper is that such things should not happen. Web presentation must be pleasing to the visitor, not to demonstrate the ability of graphic designers and programmers.

Every time we "made" a new design or create a new page, we asked questions, random to visitors: "Are you satisfied with the appearance and functionality of website?" As expected, the users were satisfied with the simple presentation with easy access to information of interest to them, while they were extremely dissatisfied with the site, which was crammed with information, slow retrieve, but was graphically polished.

Potential customer of website expects its site could be made in accordance with the latest technology, but still compatible with most browsers on the market. It will be able to exploited a long time the product we offered him.

Our recommendation for web developers is to completely turn to website development in HTML5 and CSS3 technology. HTML5 is supported by all modern web browsers and there is a large number of actual pages written in it. For example we can mention a mobile portal [www.24sata.hr](http://www.24sata.hr). The mentioned portal widely used HTML5 as the technology on which it is based.

The conclusion in one sentence is „Web presentation must be simple, affordable, done in several colors through the use of new technologies that identify the most common web browsers“.

## **6 REFERENCES**

- [1] Adobe embraces HTML5: The end of Flash as Steve Jobs predicted  
<http://tech.pnosker.com/2011/11/09/adobe-embraces-html5-the-end-of-flash-as-steve-jobs-predicted/>  
(18.3.2014).
- [2] Color  
<http://hr.wikipedia.org/wiki/Boja> (18.3.2014)
- [3] The development of HTML and new features of HTML5 standards  
<http://mapmf.pmfst.hr/~aniprl/zakljucak.html> (18.3.2014)
- [4] HTML5 - HTML for the new age  
<http://sistemac.srce.unizg.hr> (12.3.2014)
- [5] Cascading Style Sheets  
[http://en.wikipedia.org/wiki/Cascading\\_Style\\_Sheets](http://en.wikipedia.org/wiki/Cascading_Style_Sheets) (20.3.2014)
- [6] jQuery  
<http://www.tomislavdekovic.iz.hr/clanci/jquery.html> (21.3.2014)
- [7] HTML5 elements and old browsers  
<http://blog.dimedia.hr/programiranje/novi-html5-elementi-stari-browseri/> (21.3.2014)
- [8] The structure of the HTML 5 websites  
<http://mapmf.pmfst.hr/~aniprl/strukturalni.html> (22.3.2014)

## SECURITY OF INFORMATION

### EMAIL SECURITY

Hadžib Salkić<sup>1</sup>, Almira Salkić<sup>2</sup>, Amra Mirojević<sup>3</sup>, Dajana Marić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

hadzib.salkic@unvi.edu.ba, almira.salkic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba,  
dajana.maric@unvi.edu.ba,

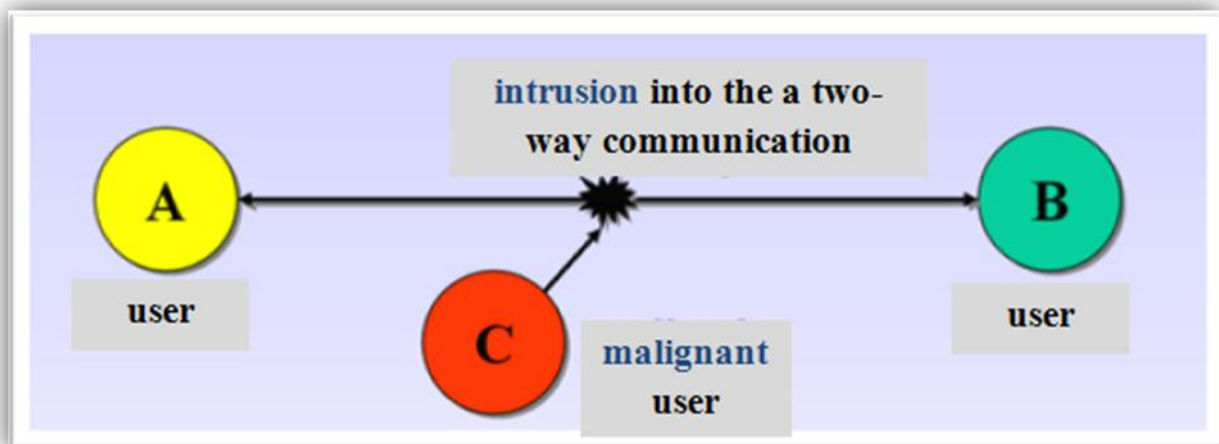
#### 1. ABSTRACT

Electronic mail is one of the most popular forms of communication on the Internet. It is also used for private and business purposes; therefore it is very important to know how e-mail is fundamentally in secure standard. Because the messages are not encrypted or protected in any way (without additional user effort), anyone with access to nodes through which messages pass, is able to read, or even worse, modify the content. In our essay we will look back on the encryption of electronic mail and the process of encryption and signing.

#### 2. EMAIL SECURITY

Electronic mail has without a doubt one of the fundamental mechanisms of communication in business environments. However, few people are aware of just how insecure emails, for example, for e-mail there is no protection for either one of the security features:

- *Availability*  
When you send a message, there is no guarantee that the message will arrive at a particular time. Given that most of the time electronic messages really come very quickly, people imply that it is permanent and then are surprised when messages are late a certain time.
- *Integrity*  
Electronic messages are completely unprotected by any changes, and the sense of the message can be changed, and it is very difficult to detect unauthorized changes (without exchanging some additional information that usually does not work).
- *Secrecy*  
Electronic messages are not secret and can only be read by anyone who has access to the communication channel, or email servers.
- *Authenticity*  
The messages are very easy to fake. Quite often we talk about some kind of „official address" which is complete nonsense if you know how email works and what problems it has.
- *Non-repudiation*  
In principle, this is not possible to full realize. There are certain scenarios where it is, but in the general case it is not possible to prove that someone actually sent the message.



Picture 4 Intrusion into the communication between two users

One of the riskier areas where they can pick up viruses and other threats is e-mail. Attachment in an e-mail is the most likely source. Sometimes just opening the message released virus.

Even if you have antivirus software, you can get to the issuance of a new virus before the last update of your antivirus software. So always be careful with attachments. Be especially suspicious if you receive a message from an unknown person (or of the person from whom you do not expect a message) or if the subject line or attachment name is weird. If you feel that the message is infected with a virus or other malicious code contains, and the sender is a friend or an associate, you can always ask for confirmation before opening. If it appears that the virus is still in the message, delete it before opening it, and then delete it from the Deleted Items folder. If you press ALT +DELETE you will delete the message completely in one quickstep.

### 3.1. What you can do:

- Get a spam filter  
It is recommended that your child create an email address from your Internet provider that offers automated virus protection and spam filtering. This way prevents most spam.
- Allow only the senders that you know  
Probably the safest, though limited, way to use the e-mail is to adjust the settings so that your child has access to only messages from specific addresses. Most of the e-mail allows blocking messages sent from specific email address.
- Consider using an anonymous-mail addresses  
Email addresses are usually name.surname @ domena.hr. Personal name is personal information and you should not publicly disclose. It is recommended that the e-mail containing a numeric value because they harder to "hit", and in this way get less junk mail. Not advisable to use the same alias twice in chat-rooms. There is a type of e-mail addresses and easier to quit if you get too much junk mail or spam. Wide permeability connections typically include several e-mail addresses.

### **3.EMAIL TRAPS**

#### **3.1.Regulations on the use of electronic mail**

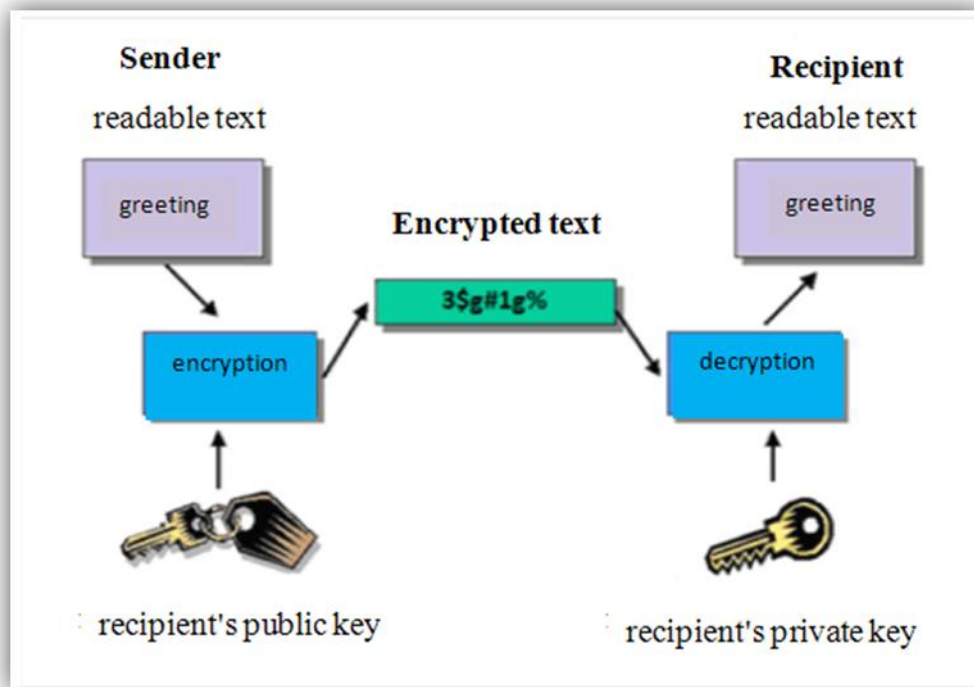
Problems which might appear when using-mail:

- The uncertainty Protocol
  - The message travels in plain text, open like postcard, and is easy to intercept and read, or even change the contents.
  - It is easy to forge the sender's address, so that you are never known exactly who sent the message.
- Accidents
  - It is always possible to press the wrong key or click the mouse on a neighboring icon. This may incur irreparable damage-you cannot stop the message that is already gone. If you pressed Reply All instead of Reply, the message instead of a single recipient to go to multiple addresses, and confidential information to reach the unwanted recipient.
  - A common mistake is when you pick the wrong address from the address book.
- Misunderstandings
  - People tend to write e-mails in casual, relaxed manner. This can lead to confusion if the other party does not understand the message in the same way. Therefore, official letters, write in an official tone.
- Disclosure of information
  - Messages intended for a single person, in no time can be forwarded to others, for example in the mailing list. This can happen:
    - a) intentionally/unintentionally, in order to harm another person or company
    - b) the negligence of the participants, who does not ask permission to forward the message
    - c) a random mistake, for example unintended click on the wrong icon (Reply All instead of Reply)
- Work Ethic
  - Chain messages that people send to acquaintances may contain false information or be part of a fraud, with intent to extort money people ("help the sufferer in need of surgery")

### **4.ENCRYPTION OF E-MAIL**

Standard for the exchange of electronic mail in the basic edition does not offer the possibility of verifying the identity of the sender. Therefore, the potential attacker able to falsely present themselves and so do harm to the user.

Encryption of e-mail is the process by which contents e-mail is encrypted and in such form transmitted from the sender to the recipient.



Picture 5 Encryption of e-mail

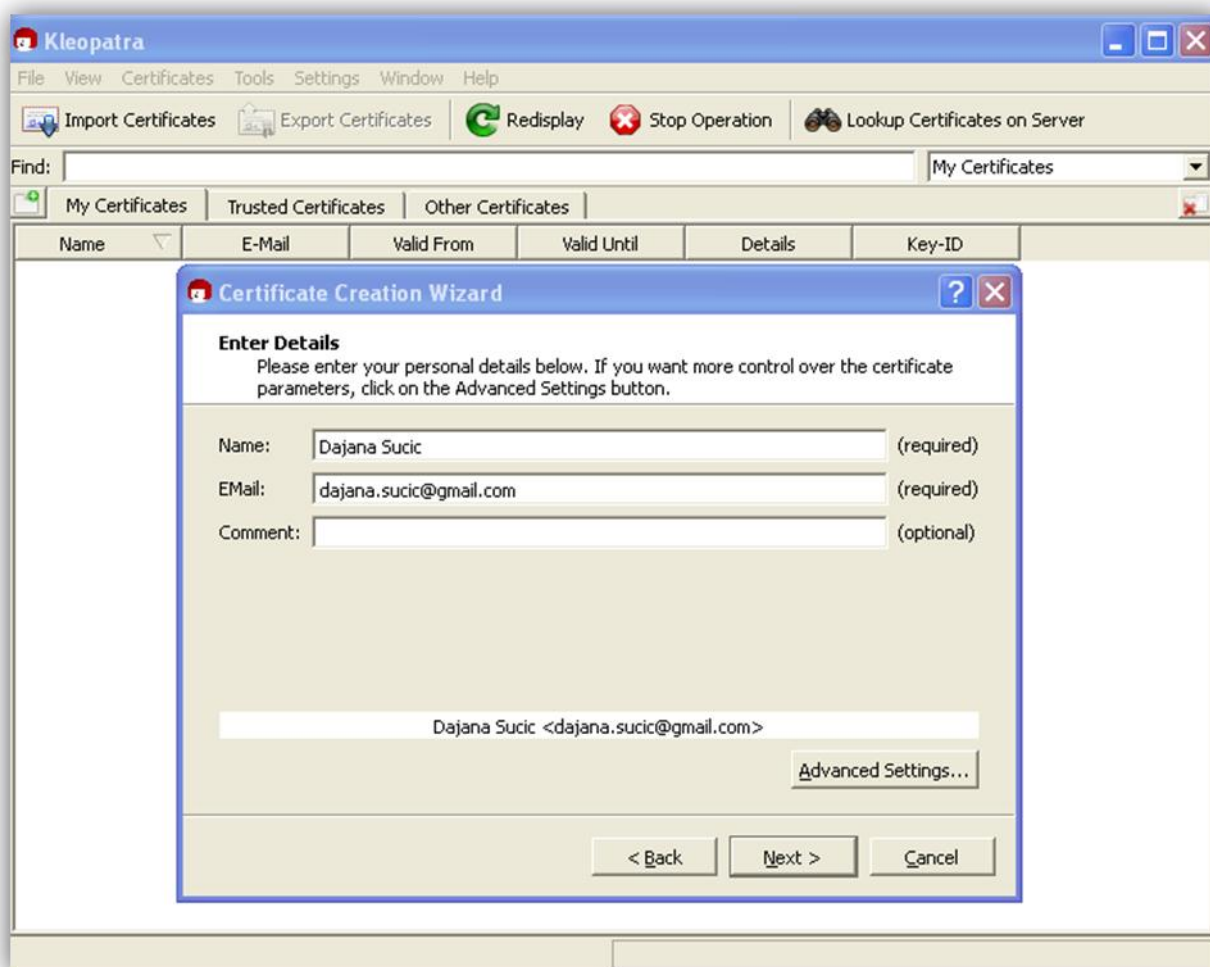
There are several methods for the encryption of electronic mail messages:

- **PGP** (Pretty Good Privacy) is standard that allows you to protect the contents mail compression procedure, and finally encryption (symmetric and asymmetric processes).
- **S/MIME** (Secure/Multipurpose Internet Mail Extensions) is a standard similar to the previous-also uses asymmetric cryptography to encrypt mail.

### 5.1. Encryption process and signing

The process begins by generating a pair of keys. The keys can be encrypted with different cryptographic procedures for the purpose of encryption and signing:

- symmetric algorithms Cast5, Camellia, Triple DES, AES, Blowfish, Twofish,
- asymmetric algorithms RSA and ElGamal,
- hash OSesRIPEMD-160, MD5, SHA-1, SHA-2i Tiger.

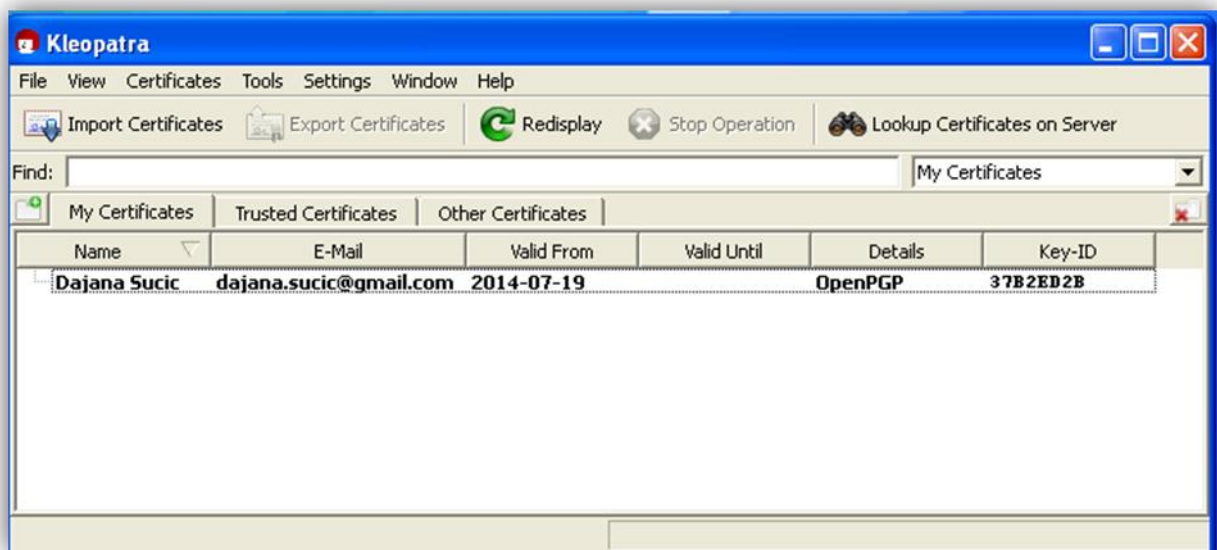


Picture 6 Generation key

Generating a key is performed by the tool Cleopatra, selecting New Certificate from the File menu and then tool the user enters basic information (name, email, password lock / unlock). A copy of the key is to log to a secure location, so that the user was not sure that his electronic identity will be preserved in case of damage by computer he use.



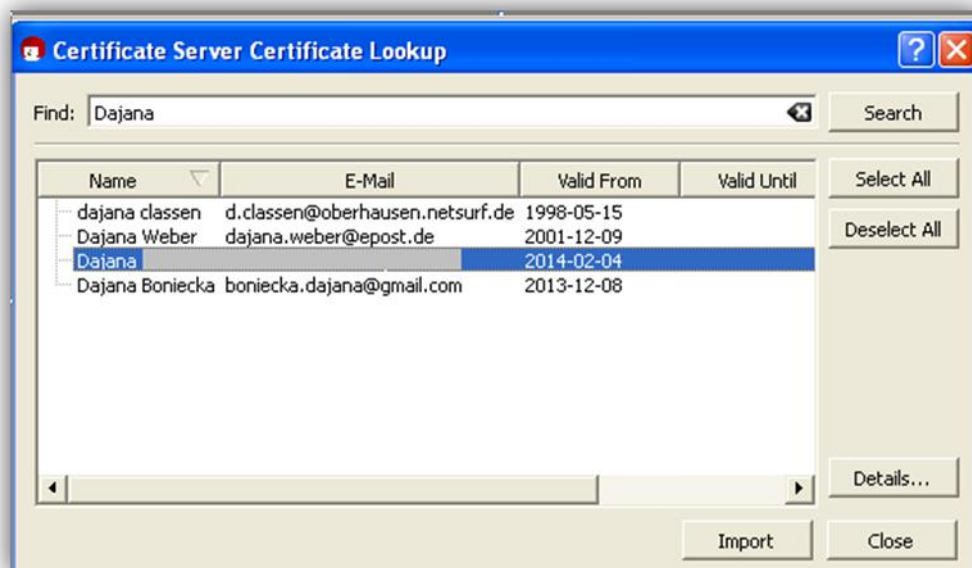
Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 7 Encryption tool-Cleopatra

In order to user be able to encrypt mail to the correct recipient, must necessarily possess the public key of the recipient. The key is possible to obtain with a public key of the server (after your recipient's public key published) or direct exchange of keys to some other channel.

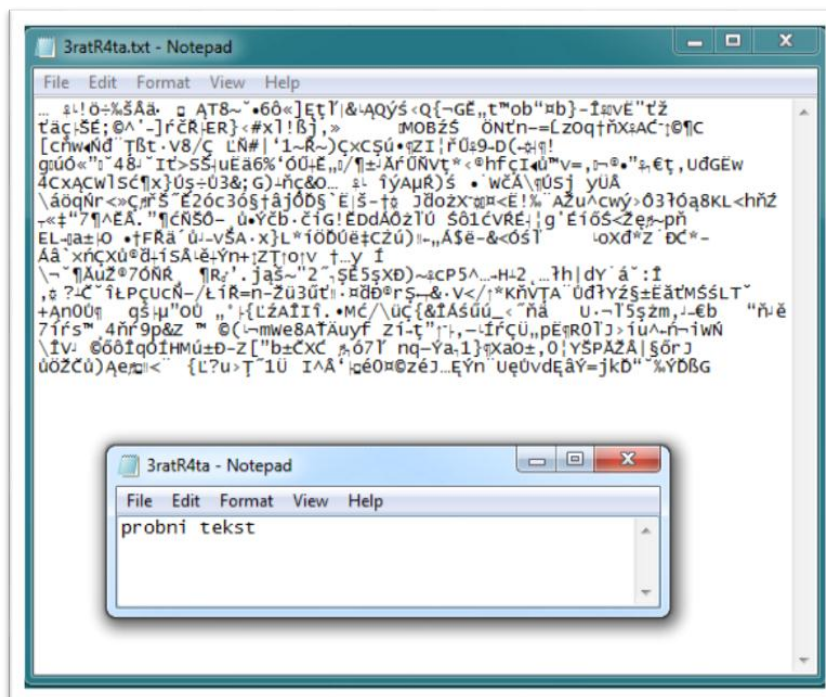
Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 8 Importing key from the server key

After the preliminary work, (generated public and private key and import your own public key recipients) need to select the Sign/Encrypt Files from the File menu.

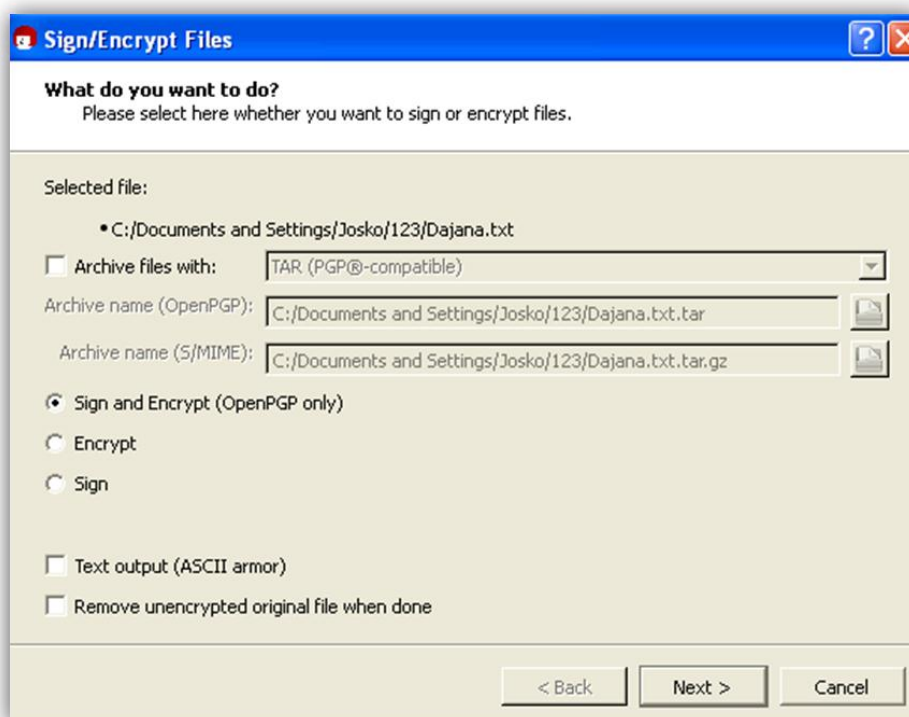
Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 9 Example of encrypted and decrypted text

After the selection files, you need to select the desired action (encryption and/or signing).

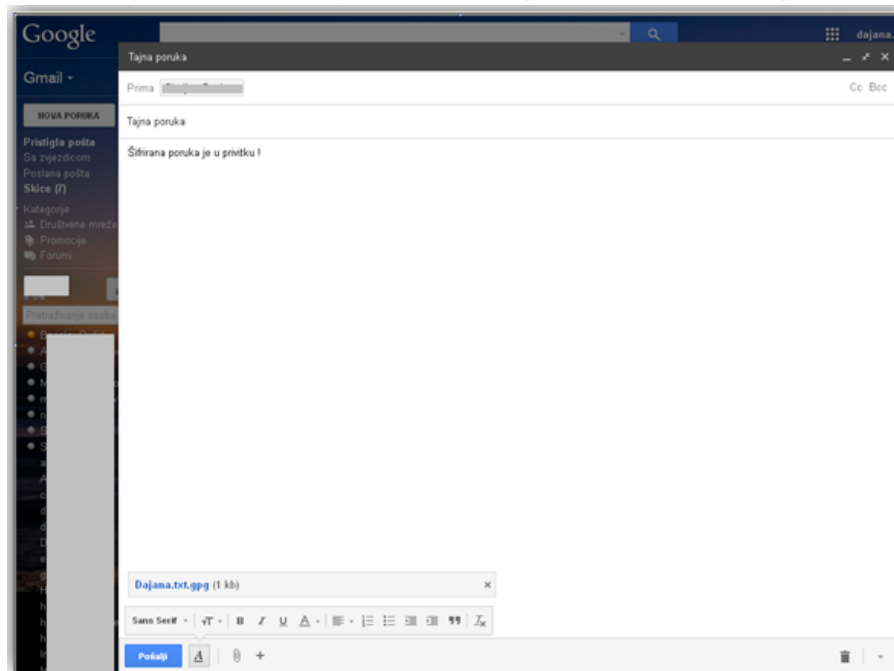
Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 10 Options of encryption/signing

Encrypted message is sent to the recipient as an attachment with a message indicating in body of the message that attachment has a confidential content. The recipient after receiving the message, in reverse process, decrypts the message. It is important to note that the decryption can be performed by any tool that supports asymmetric cryptography, and that the recipient may not necessarily use the same tool (GPG4win) as well as the sender.

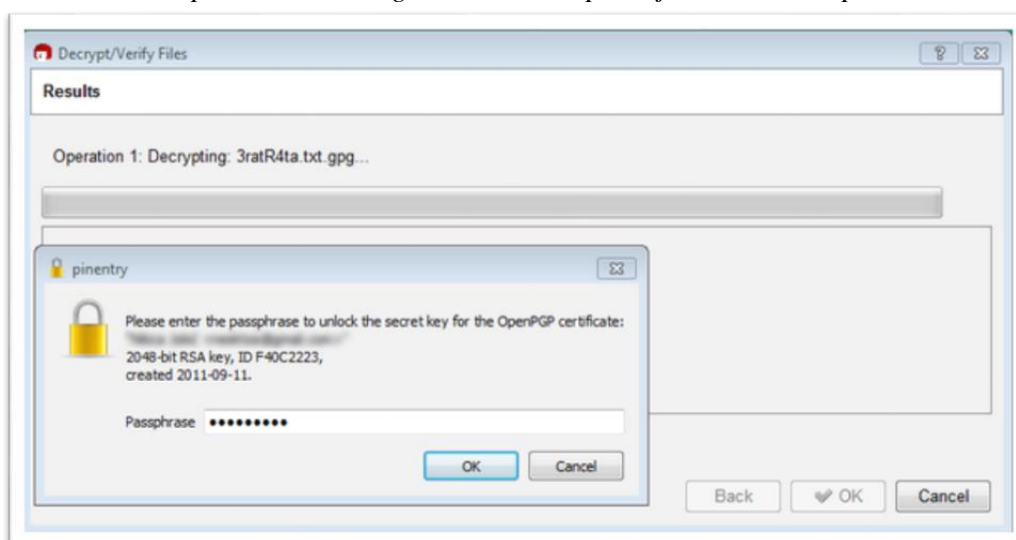
Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 11 Sending encrypted content

Decrypt messages is done by selecting Decrypt/Verify Files. It is necessary to load the encrypted file and start the decryption process.

Source <http://www.cis.hr/sigurosni-alati/kriptiranje-elektronicke-poste.html>



Picture 12 Decryption of messages

If keys meet each other, tool responds with message of successful decryption, after recipient can read decrypted message. GPG tool set is due to its long presence and stable development, and, of course, high availability as a result of the openness and the availability of procurement has become de facto standard for the exchange of electronic mail. As such it really does not equal quality and at the same time equally available and supported alternative.

GPG is actually a free open-source implementation of the PGP standard. There is also a commercial PGP software solution designed for advanced use cases (since the basic use cases covered free tools).

## **5.CONCLUSION**

Using the authentication of the sender address, with the help of public key infrastructure, it is possible to reduce traffic in spam e-mail on the way from the server to the recipient or between two servers. By enabling the classification of e-mail messages in a secure manner realized significant savings in time and prevented a possible loss of information. Using the developed system, users no longer need to spend time sorting mail and browsing that they are not perhaps mistakenly important message marked like spam message. Specifying the rejection of unsigned and signed messages incorrectly already on the server, it is possible to completely eliminate spam messages. Applying this way, the sender of the message is determined in a safe way, without the possibility of fraud.

The introduction of the wider use of secure e-mail system or a similar system based in the use of digital signature and public key infrastructure, it is possible to reduce the amount of spam in a safe and easy way, without the fear of loss information that are mistakenly considered as spam based on the content even though sender is trustworthy. Using digital signatures you reduce the extent of adverse actions such as sending spam, and identity theft as well as increasing the overall level of security in communication by e-mail.

## **6.LITERATURE**

- [1] <http://sigurnost.tvz.hr/E-Posta/> (15.03.2014.)
- [2] <http://www.cis.hr/sigurnosti-alati/kriptiranje-elektronicke-poste.html> (15.03.2014.)
- [3] <http://kristinaernjes.wix.com/sigurnost#!zamke-elektronike-pote/c12s6> (16.03.2014.)
- [4] <http://www.itsistemi.com/hr/rjesenja/sigurnosna-rjesenja/sigurnost-elektronicke-poste/> (18.03.2014.)
- [5] <http://office.microsoft.com/hr-hr/training/sigurnost-i-poboljsanje-sigurnosti-u-sustavu-2007-office-RZ010194141.aspx?section=8> (18.03.2014.)
- [6] <http://voditelj.sigurnosti.blogspot.com/2013/01/edukacija-sigurnost-elektronicke-poste.html> (18.03.2014.)

# **WIRELESS WI-FI COMPUTER NETWORK AND SECURITY WI-FI NETWORK**

Mahir Zajmović<sup>1</sup>, Arminka Šabanović<sup>2</sup>, Sidika Šabić<sup>3</sup>, Damir Pivić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

mahir.zajmovic@unvi.edu.ba, arminka.sabanovic@hotmail.com, sidika.sabic@gmail.com,  
damir.pivic@yahoo.com

## ***1. INTRODUCTION***

This essay deals with the Wi-Fi technology, application and security Wi-Fi networks. Institute of electrical and electronics engineers - IEEE International body, 1997th year brings specification 802.11, because it is observed that the government had started to happen before what began to happen in the beginning of the development of LANs. So it is the lack of standards - which led to the fact that manufacturers sell incompatible equipment. Mass acceptance standard is experienced after the 1999th when it accepts much faster 802.11b standard and 2003rd when accepting the 802.11g standard, which was first brought quite acceptable speed, as well as facilitated the growth of the city's public 802.11 networks. Minor problems with compatibility and continues to have, but certification of wireless products labeled "Wi-Fi CERTIFIED" by the Wi-Fi Alliance slowly leads to the removal of the fear of customers buying incompatible equipment. The very concept of Wi-Fi is not an acronym, but a trade name. Although initially Wi-Fi planned for use in cell phones, laptops and a similar portable devices inside the home and office, it soon became clear that the very usable for desktop computers, and is accepted by many amateurs and professionals to connect remote networks and computers without rent (mostly overpriced) leased lines.

Mainstream adoption of broadband Internet access (via cable and ADSL) comes to creating a home, small and large urban network which is one of the functions of Internet Connection Sharing. For some, this is the only way they can achieve broadband access where it is not possible - from a variety of bureaucratic and technical reasons. Unfortunately, from the point of view of security, wireless networks were a step backwards. Wired networks have an advantage because the access to the communication channel is possible only with physical access to the cable, while the Wi-Fi networks only represent a security authentication and encryption. Often (and mostly at default settings) traffic is unencrypted, while the first generation of wireless encryption, WEP, today it is possible to decrypt the stronger computer for a few minutes. Unencrypted installations pose a particular problem if the connection is charged by the amount of turnover - which resembles stealing electricity or telephone connections from neighbors.

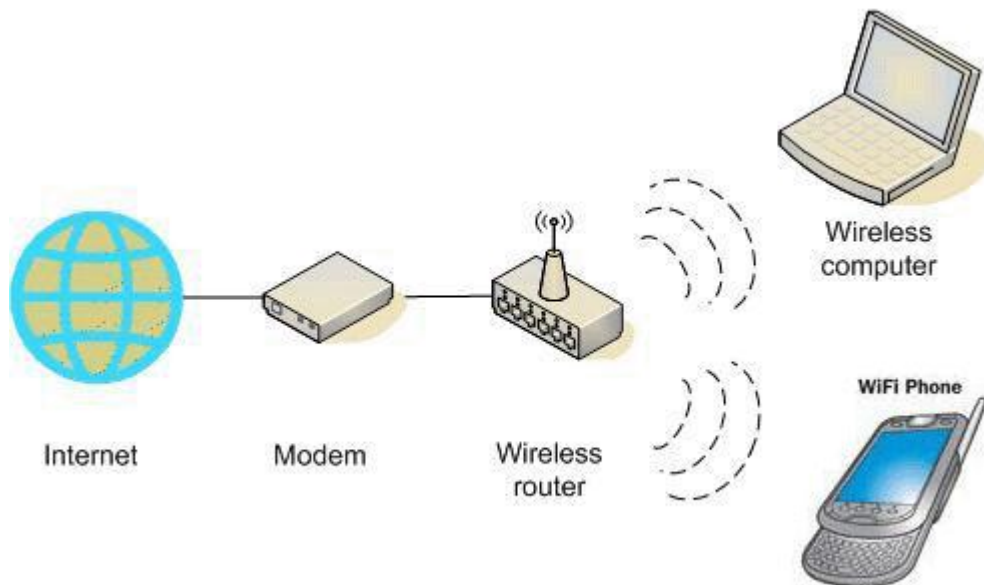
Other possible problems are common for computer network - the theft of sensitive and private information to the insinuations of viruses, Trojans, etc. The solution is to use encryption system to newer generation of WPA, WPA2, AES, and the like, which will be discussed further in the remainder of the text.

## 2. OVERVIEW OF STANDARDS SECOND Wi-Fi NETWORK



Wi-Fi, Wireless Fidelity (IEEE 802.11) wireless networks where data between two or more computers are transmitted using radio frequency (RF) and the appropriate antenna. The most commonly used in LAN networks (WLAN), but lately more and offers wireless WAN network - the Internet. Wi-Fi is a brand of Wi-Fi alliance which prescribes the standards and certifies all Wi-Fi devices. Wi-Fi in 1991 invented NCR Corporation / AT & T in Nieuwegein, the Netherlands. The first network called WaveLAN and worked at speeds of 1 to 2 Mbit / s. Father Wi-Fi is considered Vic Hayes, whose team developed the standards for Wi-Fi, such as IEEE 802.11a, 802.11b and 802.11g. 802.11a standard has a theoretical speed of 54 megabits per second, but usually it is around 30 megabits / s. This standard is more expensive because the Wi-Fi card based on the standard of work at higher frequencies (5GHz, as opposed to 2.4 GHz with big standards)

- 802.11b standard introduced 1999th at the same time as 802.11. In such networks, data speed up to 11 megabits per second, but with great obstacles and interference rate may come in small 1 to 2 megabits / sec. This is also the cheapest variant of Wi-Fi networks.
- 802.11g was launched in 2003. Year and united the two previous standards. Operate on 2.4.GHz, but has almost the same speed as 802.11a standard.



**Figure 1.** Wi-Fi networks

## 3. MODE

Wi-Fi networks operate on a very simple radio technology; the only difference is that the radio signals are converted into ones and zeros.

All radio technology is the Wi-Fi card that you can put into a computer (some newer laptops have built-in card), and it is practically all you need for wireless networking. This is why wireless networking is considered one of the simplest is currently on offer, and another reason is that eliminates the need for cables and other network devices. The only thing a user can do is to be clipped onto the so-called. hotspot, or connect the hub where other users. Usually it is a small box containing the Wi-Fi radio to communicate with other users, and it is usually a hub connected equipment on the Internet. Such nodes can already be seen in some developed cities in high-traffic locations such as parks and airports,

making it possible to have wireless access to the Internet with a laptop. Sometimes it happens interference signals on the 2.4 GHz frequency, usually with cordless phones and Bluetooth devices using the same frequency.



Figure 2. Mode

#### 4. PHYSICAL COMPONENTS

##### 4.1. CABLES AND CONNECTORS

In today's wireless connection great attention is paid to the cables - most works great differences in the flow of data between the quality of cabling and unprofessional. In networking, the following groups of connectors: connectors for connecting wireless equipment directly to a wired network or computer, the connectors on the cable to connect an external antenna to the NIC, and the power cable connectors. Importance is obvious - they tend to use shorter cables, less than 5 meters.

For greater distance, many prefer to use an external installation of equipment (with a water-tight box) to minimize losses. Obviously, the antenna cables have losses because the signal is analogue as Ethernet does - because data is transmitted digitally.

##### 4.2. WIRELESS NETWORK CARD

Wireless network cards used a computer to communicate with the AP or other wireless client. Regularly come in three versions: as a PCI card (used in desktop computers), PCMCIA cards (used in portable computers) and USB card (practical because they can be used on all computers with a USB port, and the added value it gives them the fact that they are not physically tightly linked to a computer).

##### 4.3. ANTENNAS

Antennas for WLAN can be divided into two basic groups: directed and bidirectional. Under directional antennas which are considered to be the beam spread of the signal is less than 30 °. Of course, this focus results in greater loss of signal, and the directional antenna used by the client to the



access point or placed in a point-to-point “ “ connections over long distances. These Bi-directional antennas cover a larger angle than directed and used at access points to cover a specific area of the signal.



**Figure 4.** Directional antenna



**Figure 5.** Bidirectional antenna

#### ***4.4. WI-FI NETWORK ADAPTER***

Wireless cards are wireless equivalents ordinary network card - working on the physical and data levels (1 and 2) of the OSI model. They come in a PCI version, mini-PCI, PCMCIA, USB, Compact Flash and SD cards, as well as integrated on the motherboard, for example, devices. Except

Notebooks, mini PCI and PCMCIA are often embedded in the access devices. Mainly used in infrastructure mode (for connecting to devices in master mode), in ad-hoc mode (to connect one on one), but part of the card supports and putting in master mode to connect to other clients, thereby serving as AP (mainly depends on the support of the driver). Typical parts of the Wi-Fi network cards are chipset, radio chip, and built a mini antenna or connector for connecting an external antenna.

### ***5. TYPES, SETUP WI-FI NETWORK***

Standard 802.11 provides for two basic ways of achieving interoperability: Ad-Hoc and Infrastructure (Infrastructure) modes.

- Ad-hoc (peer to peer) mode is the simplest form of wireless connectivity. It connects one device to another without the use of a base station, like connecting network devices crossover cable. 802.11 standards do not allow the use of higher speed (declared) 11Mbit. Connecting to an ad-hoc fashion as possible and to 54Mbit, which led to many manufacturers and 802.11g equipment installed option this way of connecting a configurable option. Although the legality of this is questionable, use is widespread.

- Infrastructure mode implies the use of an access device - the AP, it is a device that operates in master mode - either a factory-made device or a computer with a network adapter with software support it provides. Clients can connect to manage mode.

Other types are optional / non-standard and depend on the manufacturer of the equipment:

- Bridge mode acts as a bridge between the two AP devices, similar to an ad-hoc basis. It does not allow clients to connect devices.
- Repeater mode allows bridging as bridge mode, but with the possibility of simultaneous clients connecting to each AP. Rarely used to the difficulty, and reliable functionality can be achieved by using a computer with multiple network adapters - one in master mode, the second instance in ad hoc mode with another AP.

## 6. SECURITY WI-FI NETWORK

Due to the nature of the medium that is used for data transmission in a wireless computer network is necessary to meet additional requirements to the data flow was safe and that the network was protected from unauthorized access. To ensure the security of data exchanged over the wireless network uses some of the methods of encryption. The best known are WEP, WPA and WPA2. WEP encryption is the oldest method that is more generally not used because its mechanism is very easy to break using specialized software tools. Much safer solution is to use WPA or WPA2.

To protect the network from unauthorized access, in addition to WEP, WPA or WPA2 encryption can be used and several other methods. One of them, also the weakest, is a method of hiding the access point identifier (SSID). The family of standards for wireless communication 802.11 provides that each access point broadcasts identifier - the name of the access point. However, on most wireless access points can be ruled broadcast identifier ensures that the network is invisible to ordinary users - her name does not appear in the list of available access points. This will prevent automatic connection of computers on the first available access point to be discovered. Advanced users can use the appropriate software tools and cause the access point to respond to the call and make it so visible. Another way is to allow the access point to connect only computers whose wireless adapter has a specific MAC address. This method of protection is also inefficient because MAC addresses can be relatively easy to forge. If a malicious user knows the MAC address that is allowed to connect to a wireless point, according to this information can change the MAC address of your network adapter and no problems to connect to the network. When people explain why it is necessary to set encryption on wireless, their first thought is that someone will connect to their network and use your Internet connection. Of course, there's that, but disabling anyone to uninvited connected to a wireless network is just a side effect of the complete encryption of communication between two nodes, in this case computers and access points. No one (when it's coded) without these codes can't begin to communicate. However, the code is not just about the key that opens the door to some imaginary internet, it actually opens the door to your network and everything that goes with it, such as shared files and folders on the disks of networked computers, including Internet access.

If your Wi-Fi does not have a password, then it is the right time to make it. Way you set or you change the password is shown in the following figures.

**Step 1.** On the Start menu, type cmd, and then open the program. .



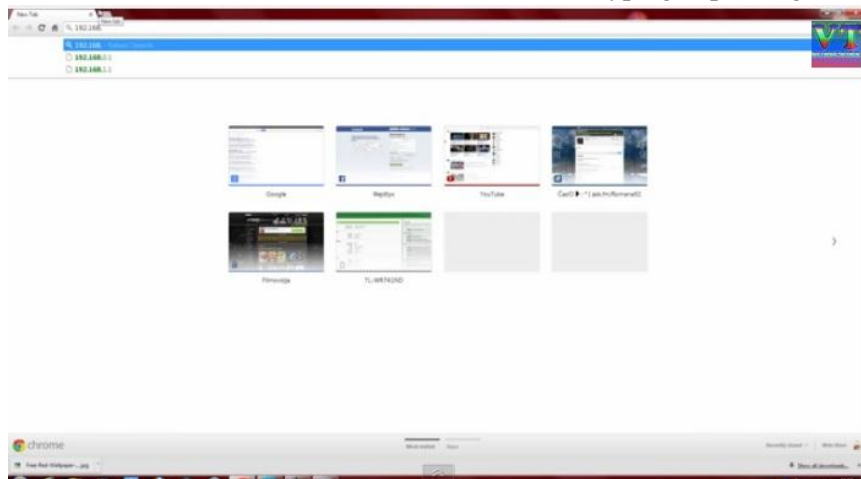
**Figure 5. CMD**

**Step 2.** In this program you type cmd IP config. Then find a number under default Gateway.



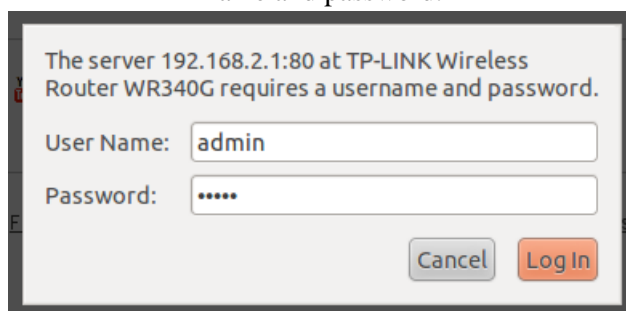
**Figure 6. Number of router**

**Step 3.** Access the router is 192.168.1.1 or 192.168.0.1 typing depending on address



**Figure 7. Access router**

**Step 4.** After accessing the address you will receive a window where you need to enter a user name and password.

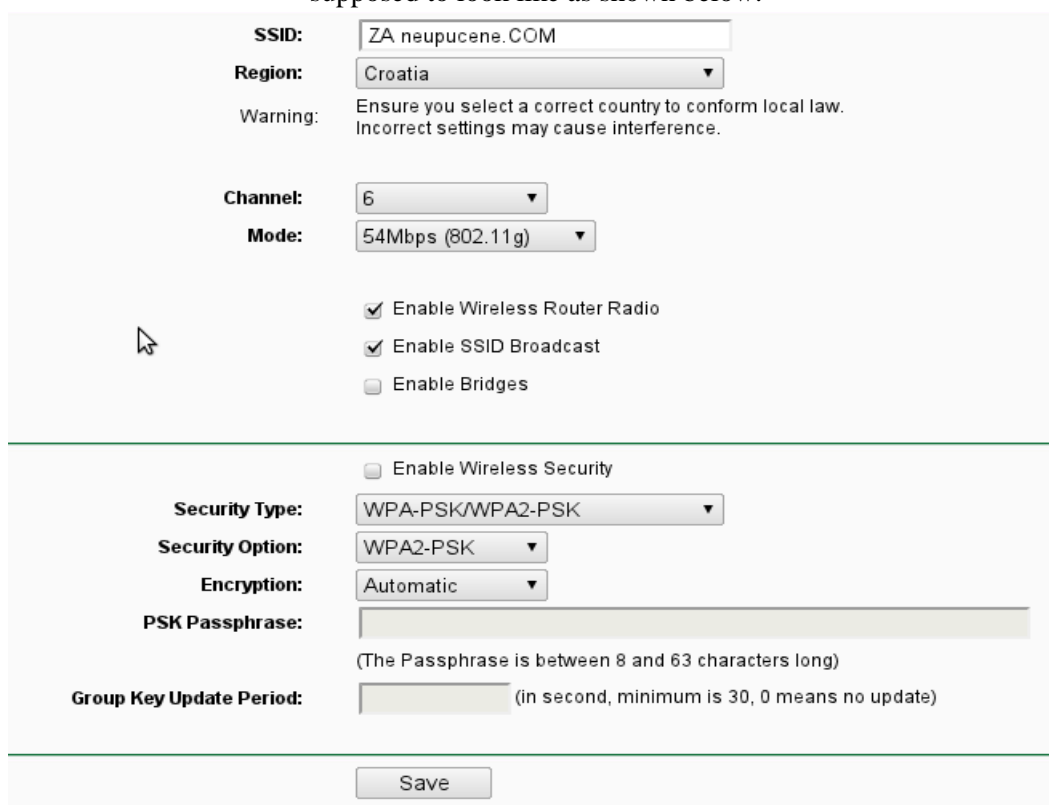


The server 192.168.2.1:80 at TP-LINK Wireless Router WR340G requires a username and password.

User Name:

Password:

**Step 5.** Once you have accessed the page it is necessary to find the Wireless section. He's supposed to look like as shown below.



**SSID:**

**Region:**

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

**Channel:**

**Mode:**

☒ Enable Wireless Router Radio

☒ Enable SSID Broadcast

☐ Enable Bridges

---

☐ Enable Wireless Security

**Security Type:**

**Security Option:**

**Encryption:**

**PSK Passphrase:**

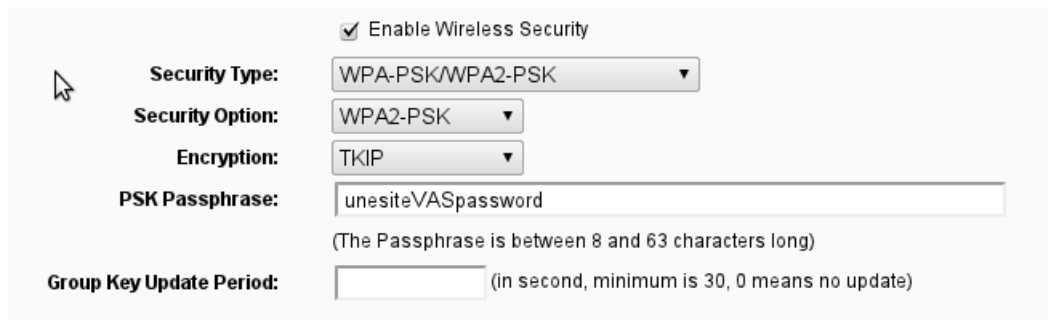
(The Passphrase is between 8 and 63 characters long)

**Group Key Update Period:**  (in second, minimum is 30, 0 means no update)

**Figure 9.** Change the password

Under SSID specified is the name of your wireless network, and then check the option "Enable Wireless Security".

**Step 6.** Select all like the picture. In the section "PSK passphrase", enter your password. It is recommended that the password don't be the same as the name of the network or if you want a stronger password; use the password generator, which you can find here.



☒ Enable Wireless Security  
**Security Type:** WPA-PSK/WPA2-PSK  
**Security Option:** WPA2-PSK  
**Encryption:** TKIP  
**PSK Passphrase:** unesiteVASpassword  
 (The Passphrase is between 8 and 63 characters long)  
**Group Key Update Period:** (in second, minimum is 30, 0 means no update)

**Figure 10.** Entering the password

**Step 7.** In the end, simply click the "Save" button and that's it. You will have a secure network and you will not be classified under the option of voting "neighbors WiFi".

## 7. CONCLUSION

Wireless networks have evolved several years of experimental technology to real usability. Unfortunately, manufacturers have opted for the replacement of wired local area networks - rather than an extension thereof. The focus is on sale to the segment of home users, and to those who have a problem broaching another cable at home. In principle, the only community of amateur unlocks the full potential of this technology - often with obstacles and manufacturers and outdated laws. Today, few modern cities exist without developed a wireless network. Check technologies such as 802.11n will certainly be help. Many start to engage with WiFi because it imagined as a cheap substitute for access to the Internet - which is mainly related to its web part. Though this possibility, city wireless is much more than that!

## 8. REFERENCES

- [1] Matthew Gast: *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002.- eBooks (13.07.2014.)
- [2] Cyrus Peikari, Seth Fogie: *Maximum Wireless Security*, Sams Publishing, 2003.- eBooks (13.07.2014.)
- [3] <http://bs.wikipedia.org/wiki/Wi-Fi> (13.07.2014.)
- [4] <http://www.howstuffworks.com/wireless-network.htm> (13.07.2014.)
- [5] <http://serbianforum.org/tutorijali/61063-recnik-wi-fi-termina.html> (13.07.2014.)
- [6] <https://www.youtube.com/watch?v=rilxcKkdJ9U> (13.07.2014.)
- [7] Quelle Bild 5, 6, 7 - Eigene (13.07.2014.)
- [8] <http://static.howstuffworks.com/gif/wifi-phone-3.jpg> (13.07.2014.)
- [9] <http://www.zaneupucene.com/kako-zastititi-vas-wifi-ruter/> (13.07.2014.)
- [10] [http://www.prejftino.com/admin/upload/pic/an6006b\\_medium\\_4dc64ff20cd44\\_350xr.jpg](http://www.prejftino.com/admin/upload/pic/an6006b_medium_4dc64ff20cd44_350xr.jpg) (13.07.2014.)

## **USE OF THE PROTECTED WEB NETWORK – SSL PROTOCOL**

Mahir Zajmović<sup>1</sup>, Alma Bešić<sup>2</sup>, Adrijana Veselinović-Dolić<sup>3</sup> i Nermina Konjalić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

mahir.zajmovic@unvi.edu.ba, alma.besic@gmail.com, adrijana.veselinovic@gmail.com,  
nermina.konjalic@unvi.edu.ba

### ***ABSTRACT***

In a present day we using Internet network regularly. Multimedia Internet network is grown up to a world network that has a large impact on our lives and since 1991st is like Panian named it as “universally goodness of humanity”.

Maybe just because of freedom that internet gives to people, dangers that they may be exposed is often overlooked. Today, like never before, anyone can become informed about some person private information's without exchange a word with that person.

Just because of that, today there are a many ways that users of internet network could protected them self, they finance or identity information's, and one of the ways is visiting of the web location secured by SSL protocol for sure.

### ***1. SSL PROTOCOL***

SSL is abbreviation for Secure Sockets Layer, what indicates transport TCP/IP protocol which enabling data encryption on the Internet and for helping web site users confirm the owner of the web site. It's used protect communications between servers on one side and clients on the other side. SSL is increasingly used for communications between two or more servers.

Encryption is a mathematical method of programing code which is coding and decoding information. Process of coding and decoding is based on several different algorithms. When an encrypted session is established, the encryption level is determined by capability of the web browser, SSL certificate, web server and client computer operating system.

#### ***1.1. SSL certificate***

An SSL certificate is a part of code installed on web server that provides security for online communications according to SSL protocol. Additionally, SSL certificate enable validation and authentication of different security levels. Also, it's verification from SSL certificate issuing company that this site is using data encryption.

Issuing of an SSL certificate depends on type of chosen certificate. Depending of client choice, SSL certificate may be issued within minutes (instant SSL certificates which is confirmed only for domain validation) take up to few weeks (SSL certificate for more domains or sub domains with additional validation). In each case, crucial for SSL certificate be issued is that all provided necessary information (including CSR file) about domain and owner are correct.

CSR stands for Certificate Signing Request and represent a file with a public key generated on server during SSL certificate implementation process. Those file content different information about server, web site and organization, necessary for issuing SSL certificate. CSR file is necessary for issuing an SSL certificate.

Every SSL certificate consist of unique pair of keys: one is a secret private key and the other one is public key. Data coded with specific public key could be decoded only with according private key and vice versa. Length and complexity of the key directly influence security – longer and more complex key is harder to hack by unauthorized user. Depending of key length, there are applied a different levels of encryption (40-bit, 56-bit, 128-bit, 256-bit). In fact, 128-bit encryption keys are unbreakable but even 40-bit encryption is very hard to break.

Depending on encryption level, validation and warranty, SSL certificate users will have more trust in security of corresponding SSL certificate, additionally some publishers which issues SSL certificate are known as more secure than others. Based on all elements different levels of certificates are recommended for different area of use.

## 2. SECURITY WITH GOOGLE CHROME

The default settings of Google Chrome for SSL security are set to middle and if there is not specific reason to change this settings it's easier to leave them as they are. To change SSL settings need to follow next steps:

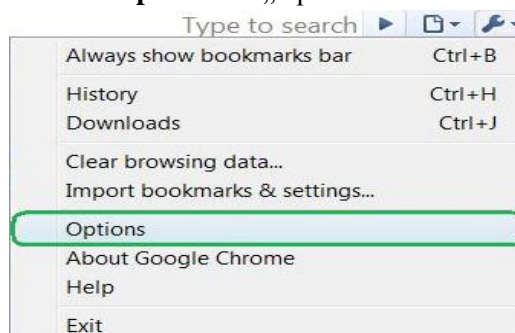
**Step 1:** Click „Customize and Control Google Chrome“

Source: <https://support.google.com/chrome>



Picture 1 Settings change,

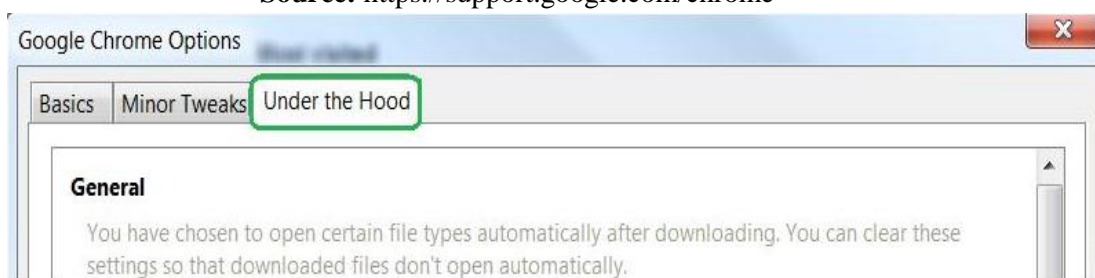
**Step 2:** Click „Options“



Picture 2 Settings change

**Step 3:** Under “Google Chrome Opt ions“ select „Under the Hood“ tab

Source: <https://support.google.com/chrome>



Picture 3 Settings change



**Step 4:** Go to „Security” and click „Manage certificates“

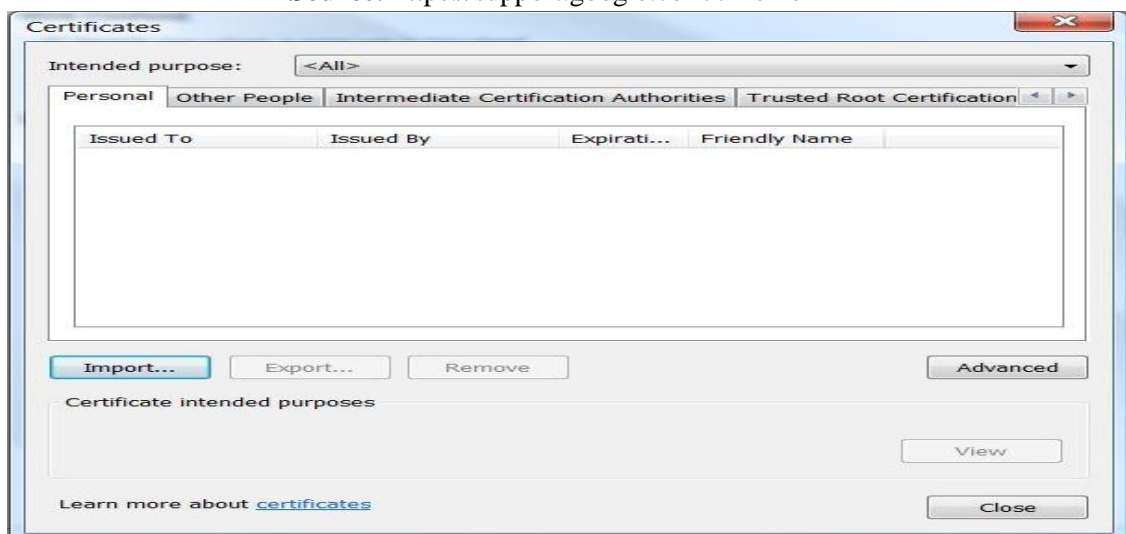
**Source:** <https://support.google.com/chrome>



**Picture 4** Settings change

**Step 5:** In window „Certificates” you can Import, Export and Remove SSL certificates

**Source:** <https://support.google.com/chrome>



**Picture 5** Settings change

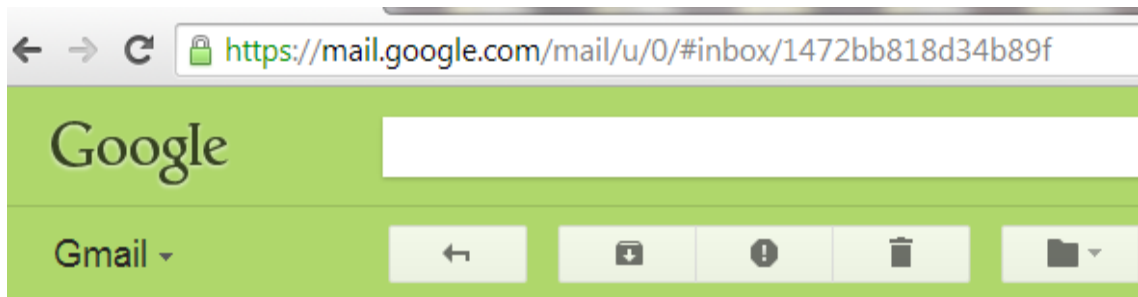
At the step 4 we could choose „Use SSL 2.0“ which is an older version of the SSL protocol that is less secure or „Check for server certificate revocation“ which issues real-time verification for the validity of a website’s certificate for extra security.

## ***2.1. Web locations secured with SSL***

Web addresses that are protected by SSL protocol are starting with https, not with http and that is a reason because someone SSL calls HTTPS. Ad Words is requiring using SSL protocol at the web sites for gathering personal or financial information. Using SSL protocol is enabling high level of privacy and security from an encrypting internet connection.

At the most of web sites is displays icon of lock when it's established SSL connection and that is most easiest way to check of using SSL protocol.

Source: Personal







Picture 6 SSL connection at web location

Google has introduced a full SSL encryption on its search services what allowing users possibility of achieving a secure connection when searching on internet. Encryption creates a secure channel that prevents third parties from intercepting and reading the data.

When connecting to some web site, Google Chrome can show details about connection and alert if it can't establish fully secure connections with the site. If on the page need to entering sensitive personal information, it's necessary to check for a lock icon to see if the site uses SSL that provides an encrypted tunnel between computer and the web location.

Source: <https://support.google.com/chrome>

Icon	What it means
	<b>The site is not using SSL.</b> This icon displays for http:// sites. Most sites do not need to use SSL because they do not handle sensitive information. Avoid entering sensitive information, such as your credit card information or bank login information, on the page. If sensitive information is being requested on a site not using SSL, consider contacting the website owner.
 https://	<b>Google Chrome has successfully established a secure connection with the site.</b> Look for this icon and make sure the URL has the correct domain, if you're required to log in to the site or enter sensitive information on the page. If a site uses an Extended Validation SSL (EV-SSL) certificate, the organization's name also appears next to the icon in green text.
 https://	<b>The site uses SSL, but Google Chrome has detected insecure content on the page.</b> Be careful if you're entering sensitive information on this page. Insecure content can provide a loophole for someone to change the look of the page.
 <del>https://</del>	<b>The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate.</b> Do not enter sensitive information on this page. Invalid certificate or other serious https issues could indicate that someone is attempting to tamper with your connection to the site.

Picture 7 Details about connection

If Google Chrome detects that some web location could be harmful for computer he shows a warning message.

Source: <https://support.google.com/chrome>





Warning message	What it means
This is probably not the site you are looking for!	This message shows when the URL listed in the site's certificate does not match the site's actual URL. The site you're trying to visit may be pretending to be another site. <a href="#">Learn more about this warning</a>
The site's security certificate is not trusted!	This message appears if the certificate was not issued by a recognized third-party recognized. Since anyone can create a certificate, Google Chrome checks to see whether a site's certificate came from a trusted organization. <a href="#">Learn more about this warning</a>
The site's security certificate has expired! or The server's security certificate is not yet valid!	These messages appear if the site's certificate is not up-to-date. You could see this message when your computer's clock is incorrect. Therefore, Google Chrome can not verify that the site is secure.
Cannot connect to the real ...	This message appears when a site is suspected to be unsafe.

Picture 8 Warning message

## 2.2. Security certificates and security of web location which is using SSL

Web location that using SSL present security certificates to the browser to verify their identity. Anyone can set up a web pretending to be another site, but only the real site possesses a valid security certificate for the URL. Invalid certificates could indicate that someone is attempting to tamper with connection with the site.






Source: <https://support.google.com/chrome>

Icon	What it means
	The site's certificate is valid and its identity has been verified by a trusted third-party authority.
	The site has not provided the browser with a certificate. This is normal for regular HTTP sites (look for the  icon in the address bar), because certificates are usually provided only if the site uses SSL.
	Google Chrome has detected problems with the site's certificate. You should proceed with caution because the site may be pretending to be another site in order to trick you into sharing personal or other sensitive information with them.

Picture 9 Security certificate

Google Chrome lets you know whether connections is fully encrypted, if connection is not secure, the third side might be able to see or tamper with the provided information on the site.



Source: <https://support.google.com/chrome>

Icon	What it means
	Google Chrome has successfully established a secure connection with the site you're viewing.
	Your connection to the site is not encrypted. This is normal for regular HTTP sites (look for the  icon in the address bar).
	Your connection to the site is encrypted, but Google Chrome has detected mixed content on the page. Be careful if you're entering information on this page. Mixed content can provide a loophole for someone to manipulate the page. This content could be third- party images or ads embedded on the page.
	Your connection to the site is encrypted, but Google Chrome has detected mixed scripting on the page. Be careful if you're entering personal information on this page. Mixed scripting can provide a loophole for someone to take over the page. This could be content third-party scripts or videos embedded on the page. If you're connected to the Internet via a public wireless network, mixed scripting is risky especially because wireless networks are easier to tamper with than wired networks.

**Picture 10** Connection security

Google Chrome show did you ever visited some site before too , if it's not cleared cache and cookies cause the visited history in that case is also cleared.

Source: <https://support.google.com/chrome>

Icon	What it means
	You've visited the site before, so chances are you trust this site.
	You've never visited this site before. This message is normal if you know this is true. However, if the site looks familiar and you did not clear your browsing history recently, it may be pretending to be another site. Please proceed with caution.

**Picture 11** History of visited web location

Most of users of internet that using them at recreation purpose, if want to avoid consequences of disturb their own privacy and identity, have to think about secure if not at other ways then at lees secure them self to visited web location secured by SSL protocol.

### 3. *EPILOGUE*

How much we should care to protect our own privacy on internet we can see from the huge number of places that is talking about contents for understanding and solving problems of security at internet. Using internet could be dangerous and has a lot of risk - from breaking privacy and making inconvenience to user till different money cheating or stealing identity.

Even there is a lot of risk that users are exposed at internet networking, with a developed conscience of necessary to protect they own integrity and proper measure of protection internet is ensuring progress in safety for individual and society.

#### **4. LITERATURE**

- [1] <http://web.efzg.hr/dok/kid/BogatstvoInterneta.pdf> (July 12, 2014)
- [2] [www.sigurnost.info](http://www.sigurnost.info) (July 12, 2014)
- [3] [www.moj-ssl.com](http://www.moj-ssl.com) (July 12, 2014)
- [4] [http://www.siq.hr/ocjenjivanje\\_sustava\\_upravljanja/sigurnost\\_informacija/](http://www.siq.hr/ocjenjivanje_sustava_upravljanja/sigurnost_informacija/) (July 12, 2014)
- [5] <http://www.kvalis.com/o-portalu/item/111-sigurnost-informacija-imperativ-opstanka> (July 13, 2014)
- [6] <https://support.google.com/chrome> (July 13, 2014)
- [7] <https://www.globalsign.eu/ssl-information-center> (July 13, 2014)
- [8] <http://www.kvalis.com/> (July 13, 2014)

## ESSAY ON INFORMATION SAFETY

Amela Begović<sup>1</sup>, Hadžib Salkić<sup>2</sup>, Amra Mirojević<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

amela.begovic@gmail.com, hadzib.salkic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba

### **ABSTRACT**

*As we already know, the problem with privacy and safety is not only related to the Internet. The root of the problem had emerged even sooner. It had developed from the first cameras all the way to tagged photos on Facebook. It is difficult to define privacy in the right way. A lot has been said about the advantages of social media, but the other side of the medal should also be taken into consideration. In this case it is jeopardizing of individuals' privacy, which expose them by being generous in sharing information.*

### **1. INTRODUCTION**

As we already know, the problem with privacy safety is not only related to the Internet, either did it start with it. The root of the problem had emerged even sooner. It had developed from the first cameras all the way to *tagged photos* on Facebook. It is difficult to define privacy in the right way. The above-mentioned question should be a reason for concern. How can privacy exist today, when Facebook knows all what one did in the last years from the very moment one joined Facebook.

In order to prepare for writing this text I observed my Facebook profile and tried to look it through the eyes of other people; from my friends' perspective - who also have access to my data. I realized that a big part of my life is represented as an open book, available to everybody to read and access my information.

If someone wanted, they could exactly find out what I did in the past couple of months, not only gaining information on what I did each day, but also where and at what time.

It is strange to think about that and a little bit scary. People I have as friends on Facebook, will still be having access to my information, even if we stop being Facebook friends in the future.

### **2. PROBLEM OF INTERNET SAFETY**

#### **2.1. Does privacy still exist in the 21<sup>st</sup> century?**

Every time brings some changes, and the 21<sup>st</sup> century brought something that moved the boundaries. New technologies, the sweetest of all benefits of the 21<sup>st</sup> century, facilitated our lives and work. We benefited in terms of information, mobility, time and everything else that the new challenges of modern business and way of life seemed to jeopardize. New technologies contributed to a faster life style, e.g. enabling me to send this very text to my professor by e-mail, while once I would have had wasted more time by walking to the university and back.

## **2.2. And then came Facebook**

Life consists of various moments, various people and stories, which become parts of our past and live in the future through our memories.

Facebook defeated time and space in a way. It seems to have gathered all people at one place causing the *wow effect* so many times, e.g. when someone finds us on Facebook we have not seen in a long time. What makes Facebook super popular is that with over 500 million users, Facebook became the hot spot for communication with our friends, whether they live next to us or across the world.

## **3. WHY DID NOT CELL PHONES AND E-MAILS CONNECT US LIKE FACEBOOK?**

Cell phones and e-mails did connect us to a certain extent, but they required additional activities, i.e. asking for phone numbers or remembering e-mail addresses, which is not as easy as remembering names of school friends, which is enough for us to know to find them on Facebook.

Somewhere I read a good comparison which says that social media are indeed a diary that we never were fond of writing. That is true. All of us and our friends leave activities behind us that remain registered; just instead of letters on a piece of paper we have photos, video recordings, status updates and comments.

Looking at our Facebook photos or status updates we can precisely recur what we did in a certain period of our life: what we thought, what mistakes we made and generally what kind of persons we were. These are the reasons why people easily connect to this web site and why many feel free to say that they love it and are addicted to it, making a distinguishing Facebook from other sites.

### **3.1. Facebook is also used for business purposes**

A vast number of users of social media led to the fact that companies started to take them more seriously. Advertisers made a step further in *one to one* marketing since companies can precisely target specific groups on social media. A bunch of information that individuals reveal about themselves like age, location or personal interests represent incredibly valuable data for someone launching a company by significantly reducing their marketing costs.

*Word of mouth* marketing realizes its full potential on social networks, firstly as a communication service, given that activities involving a brand can significantly contribute to a company's business, as friends are the ones we mostly ask for advice when making a decision which product/service to choose.

## **4. WHERE DOES THE PROBLEM EMERGE?**

Everything we share with our friends rarely stays *between us*, since photos, status updates, links and posts are almost always visible to others, even to those we do not want to have insight in our activities. All these information remain on the Internet for days.

The option to refuse to use the Internet and to create a digital identity is still there, but, even if one is not concerned with the Internet, the Internet is already concerned with the individual. Even if a person is not officially on Facebook, probably some of their friends posted a photo of



them or mentioned them in a post. Sometimes it is just the case that they might refer to someone with the same name, and it is not exactly the person one wants to be mixed up with.

Today they say if you are not on the Internet you do not exist. The fact that one does not have a digital identity, may imply that one is illiterate in terms of information and informatics or that one has not recognized the advantages of the Internet.

It is better for us to watch what we say and to control what is said about us. Our goal should be to monitor our digital identity in order to show only what we want to be shown, and to mitigate what we are not fond of. With a careful development of a positive online identity and image one can contribute to the development of one's own credibility in private, as well as in business life.

#### ***4.1. Privacy in jeopardy***

A lot has been said about the advantages of social media, but the other side of the medal should also be taken into consideration. In this case it is jeopardizing of individuals' privacy, which expose them by being generous in sharing information. The main problem is that individuals themselves distribute information, neglecting privacy settings, despite their advancement level. From identity and personal data theft to jeopardy by revealing your location, privacy became topic number one among social media protestors.

On the other side, one will often hear negative comments on revealing private data for marketing purposes. *One to one* marketing sounds like the dream of all advertisers, but it can be used as a tool to manipulate eventual users. Unfortunately, this does not only concern social media, but the Internet in general, and how far it will go remains to be seen.

A scarce number of users is concerned about their safety, security and privacy within the network. An earlier version of Facebook used to protect minors by making their profiles visible only to their friends. This option does no longer exist on Facebook. Even if we do not consider the worst options, like criminal activities (bearing in mind that everybody is liable to become a victim), one should be concerned about privacy options.

Some people do not allow other users to view their friend list, while others do not hide anything and leave everything *public*. Regarding this subject matter, one should not simply consider it a matter of taste.

#### ***4.2. You and the Internet- friends or enemies***

Depending on the level of carefulness, individuals can only partially mitigate the damage and protect just a part of their privacy. Activities like opening the web browser, entering a word in *search* or opening a web site reveal information about the person using it, even though no one asked for their name and surname.

Things become even worse when one logs on an Internet service like Facebook or Myspace. By doing so, the person allows those services to gather a long list of information, which they can use for purposes of advertising, internet statistics and others. If one has not undertaken certain measures to keep their privacy, companies such as Google know their identity, from where they log in, what websites they visit, their social contacts, what they buy over the Internet and others. It is necessary to point out the bad side- there is no possible way to completely protect ones privacy on the Internet, unless undertaking extreme measures. At least one can reduce the number of private data exposed while on the Internet.

Firstly, most of the web sites an individual visits can leave a *cookie* on their computer; a file that enables an insight in how often one visits a certain web site. *Cookie support* can be removed from any web browser, but in that case visits to a half of web sites will be disabled to the user.

There is not much left to do, except to avoid certain web sites that are known for their aggressive use of the *cookie file*. A similar rule applies to web browsers, which can follow IP addresses (a series of 12 numbers that unambiguously can identify your computer on the Internet), time of search, key words used and others.

Things get more serious when one actively starts to share personal data. For example, the social network Facebook requires users to enter their real name and surname. Photos, messages and other data one shares on social media and other services can easily be found through *Google search*. Even e-mails are not safe. In certain circumstances the Internet provider may transfer individuals' data to authorities (this depends on the country one lives in and the e-mail service one uses).

Similarly, this also applies to other data that one might consider private, e.g. when opening an Internet domain one will be asked for true data, including name, last name and address which will be public (if not specifically asked and paid for privacy) and available on various services. Eventually, one has to deal with the most serious privacy threats like viruses and other malicious programs aimed at stealing passwords, credit card numbers and other sensitive information and their transfers to distant addresses.

The question is how to protect oneself. People display their data even if it is not absolutely necessary. The problem arises when users, unaware of the risk, use the same password for all web sites they visit.

Firstly, one should avoid displaying personal data if not absolutely necessary. Even if one gives away their personal data, they should use different passwords when visiting less important web services. Anti-virus programs are recommended as well as the latest versions of web browsers (like Firefox and all other recent web browsers, since they have a decent protection level against malicious web sites), avoidance of suspicious web sites, especially those offering free software or adult content. Firewall and anti-spyware are also highly recommended.

If it is inevitable to register on a suspicious or less important service, one-time-basis e-mail addresses should be used just for the purpose of registration and to avoid spam mail. One such service is the Mailinator. It is not recommended to display data one wants to keep private on social media and other services, which offer exchange of messages, photos and other data. For example, if one uploads a photo to Facebook, Facebook has the right to use it for its own purposes, without asking for permission. Luckily, nowadays, big companies like Google or Facebook have to take into consideration their users' privacy, and one should always familiarize with such services and view the possibilities that are offered. A good example is Facebook, which enabled extremely detailed options of security and privacy settings. Often users neglect those options and leave their profiles *public*, not knowing that each of the 160 million Facebook users can see their data.

One should also bear in mind, that the Facebook options enable users to protect themselves against other users, but not against Facebook itself. When reading *user requirements* carefully, one realizes that the only way to protect oneself is to not use Facebook at all, neither any other online services. Also, many of these services enabled the option to change privacy settings, but the settings are not solely sufficient, therefore every online application used (e.g. Gmail, Myspace, Flickr) should be carefully observed regarding the change of privacy options.

## **5. FIVE MOST COMMON ERRORS REGARDING E-MAIL SAFETY**

### **5.1 Using only one e-mail account**

At least three e-mail accounts are recommended to e-mail users. The business account should be used exclusively for business- related conversations. The second e-mail account should be used for personal conversations and contacts and the third one for general hazardous e-mails one receives, which means that this e-mail should be used for newsletters subscription. At the same time, if one needs an online e-mail account for example for a personal blog, the third e-mail account should be used.

The first two e-mail accounts may be free or not, while the third account should always be free as Gmail or Yahoo. An account should be changed every six months to avoid spam mail in case one's newsletter manager decides to sell their name or steal their e- mail address.

### **5.2. Forgetting phones as an options**

One of the most significant lectures in e-mail security is that one will never be completely safe, regardless of measures undertaken to secure e-mail accounts, especially when using public computers. Unless you really have to send snapshots, or communicate across the world, better think about a simple phone call before sending an e-mail. Even if a phone call can last longer for several minutes than to quickly access the e-mail account on a public computer, a phone call is a far safer option and does not leave a written trail.

### **5.3. Usage of unsecure e-mail accounts for sending and receiving sensitive corporate information**

Big corporations invest large sums of money in order to secure their computer networks and e-mails. Despite their efforts, careless employees use their personal e-mail accounts and hence jeopardize their company's businesses. Therefore one needs to protect oneself in order to avoid transferring their company's data via personal computers or personal e-mail addresses.

### **5.4. Forgetting to erase hidden files, history and passwords from browsers**

After using public computers, it is important to erase the hidden files, history and passwords from the browser. Many browsers automatically save addresses of web sites visited, and some of them remember passwords and personal data one entered, in order to help with filling out similar forms in the future. If these information end up in the wrong hands, they might be stolen. It is important that Internet users are aware of the fact that erasing hidden files on public computers erases private information too, before hackers get an opportunity to steal them.

### **5.5. Logging out without exiting the browser**

When checking e-mails in the library or in an Internet café it is often the case that the user logs out when done, but it is highly advised to completely exit the browser. The reason is that certain e-mail services show the user name (but not the password) after one logs out.

New technologies brought changes. They changed the way of life and business, as well as the perception of reality to a certain degree. Our lives became virtual, we live in a virtual world that

became our second home- that is where our friends are, as well as where we do our work and relive our boredom, but it is also a place where we encounter problems.

New technologies enabled us to educate ourselves, to share our personal experiences with others, to look at photos of inaccessible destinations, to know everything about everyone, but yet not to know anything.

All of these activities we do, we do innocently, not thinking about the consequences, going with the flow that sometimes leads us to scams and the criminal world. We do not know how to handle that flow, and the question is if it can be handled. We enjoy the flow, comment on our friend's photos, exchange comments with them and share our privacy with strangers, which belongs less and less to us.

## **6. CONCLUSION**

The Internet has opened up a whole new world to people of all ages and abilities. Real-time communication with friends in all parts of the world is now commonplace and easily carried out with e-mail, chat and other Web-based tools.

Finding and making friends online using social networking Web sites such as MySpace and Facebook has almost become a rite of passage. Students at universities around the world chronicle their lives by building online profiles and sharing personal information, photographs, and opinions in order to connect with new people. If you use one of these sites to stay in touch, to express yourself openly, and to find like-minded people, that's great. Just be sure you stay smart and safe in the process.

## **7. REFERENCES**

- [1] Michael, L.: Security Management For Occupational Safety, CRC Press,
- [2] [http://www.utexas.edu/its/secure/articles/social\\_networking.php](http://www.utexas.edu/its/secure/articles/social_networking.php) (18.08.2014.)
- [3] [http://www.pcworld.com/article/195884/how\\_to\\_keep\\_your\\_privacy\\_safer\\_on\\_facebook.html](http://www.pcworld.com/article/195884/how_to_keep_your_privacy_safer_on_facebook.html) (23.08.2014.)

## **DATA PROTECTION USB MEMORY STICK USING THE TRUECRYPT PROGRAM**

Hadžib Salkić<sup>1</sup> Adin Lemo<sup>2</sup>, Amela Haračić<sup>3</sup> i Fatima Husejnović<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

hadzib.salkic@unvi.edu.ba, adin.lemo@gmail.com, amela.haracic@gmail.com,

fatima.husejnovic@gmail.com

### ***1 INTRODUCTION***

Information is required and valued commodity in modern world. That is assets that must be protected from unauthorized access. Information is subject to a greater number of threats are very vulnerable. These days, information is mostly written in electronic form. The protection against specific threats usually costs less than a security incident.

The theme of seminar work is to protect the USB memory stick or data stored on stick. In multitude of applications that can be quite expensive and I decided open source TrueCrypt application for protection of frequently used information supplement ,toys and useful items such as a USB memory stick.

### ***2 TRUECRYPT***

The application is quite simple for those who have knowledge in informatics After installing the software on a USB memory stick we need to create a virtual disk on which we store informations. Disc can be accessed on any computer so you mount the virtual disc in which we have chosen to enter to password.

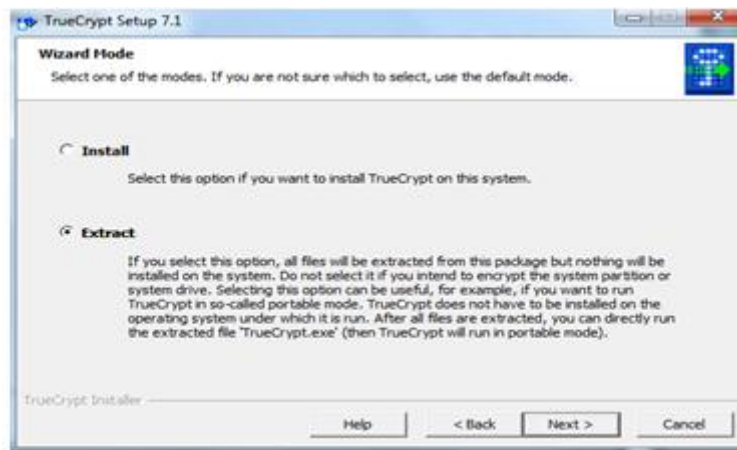


**Picture 13** Installing TrueCrypt application

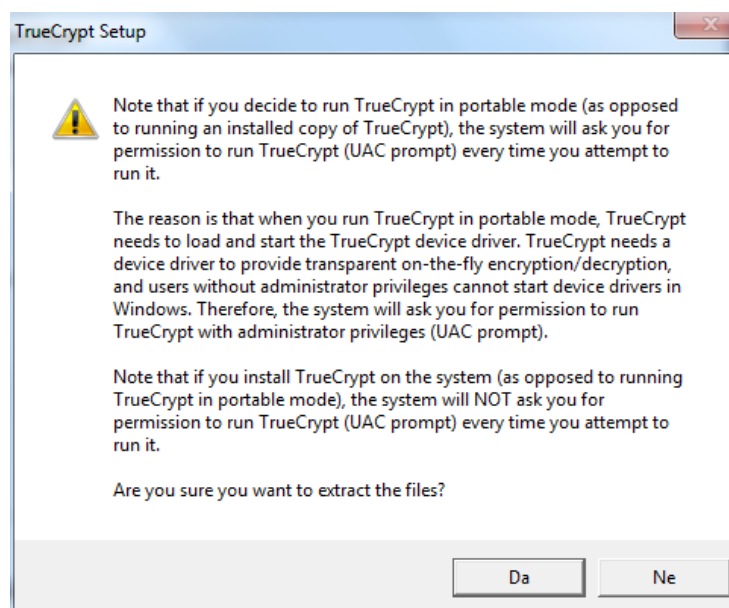
Installing TrueCrypt application is standard. Procedure is the following: Remove the program TrueCrypt on page: <http://sourceforge.net/projects/truecrypt/files/TrueCrypt/TrueCrypt-7.2.exe/download>.

### ***3 USE OF THE TRUECRYPT***

The exception is that the program extracts on the transmission medium, in this case a USB memory stick. The following windows will appear:

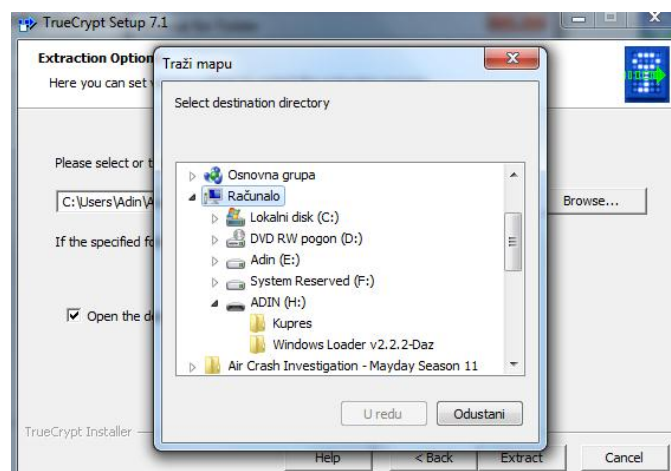


Picture 14 TrueCrypt Setup – Wizard Mode



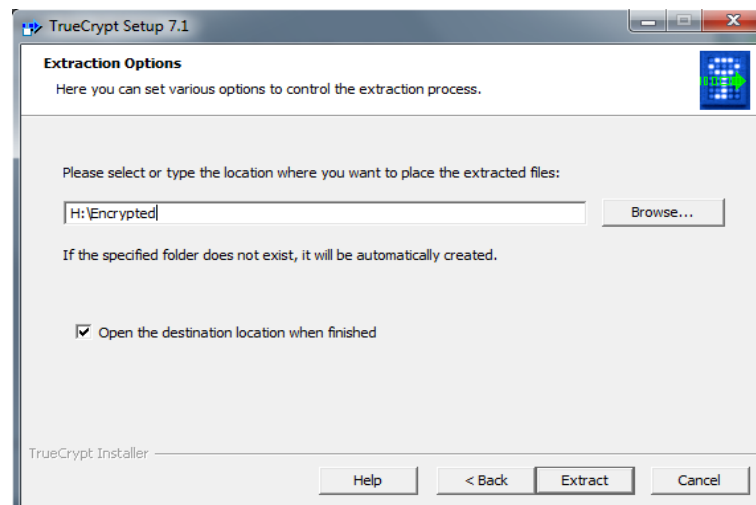
Picture 15 TrueCrypt Setup

In our case, the extraction is done on a USB memory stick called ADIN (H:)



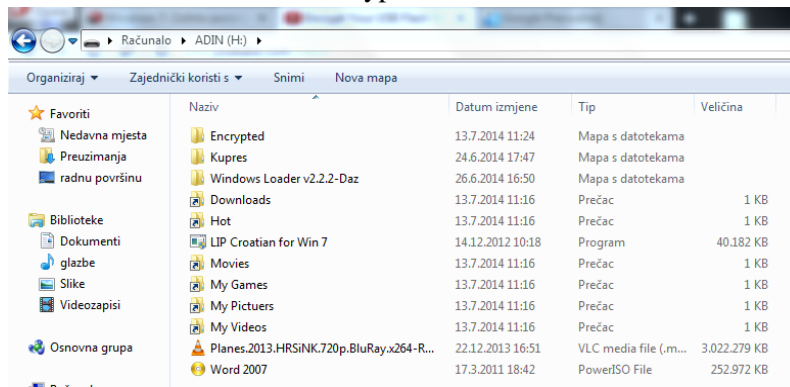
Picture 16 Extraction on USB stick ADIN (H)

Choose a file name (for example, Encrypted).



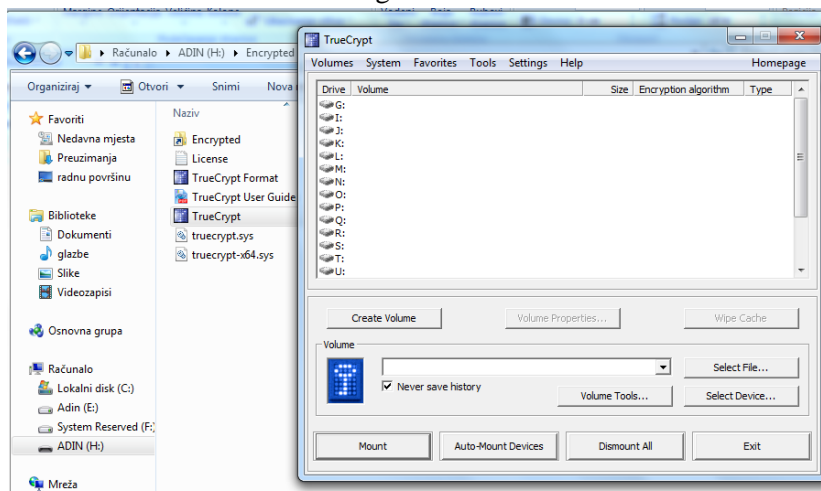
Picture 17 Extraction Options

After we click 'Extract' the installation is complete when we click 'Finish'. The picture shows that we have to stick Encrypted file:



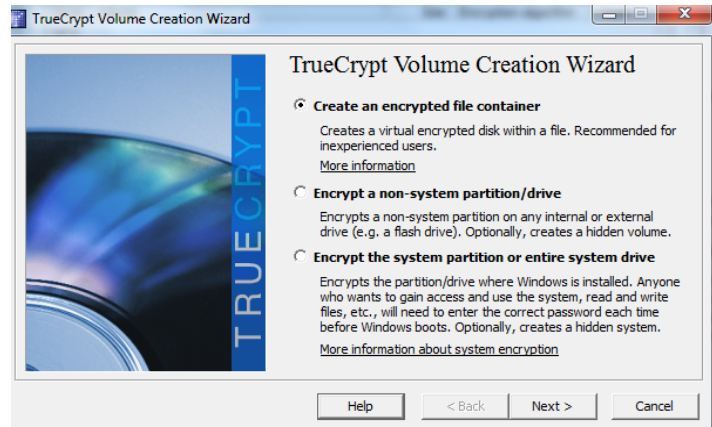
Picture 18 Encrypted file

In Encrypted TrueCrypt.exe click a file and a window will appear. In that window you should click 'Create Volume'. We have the following:

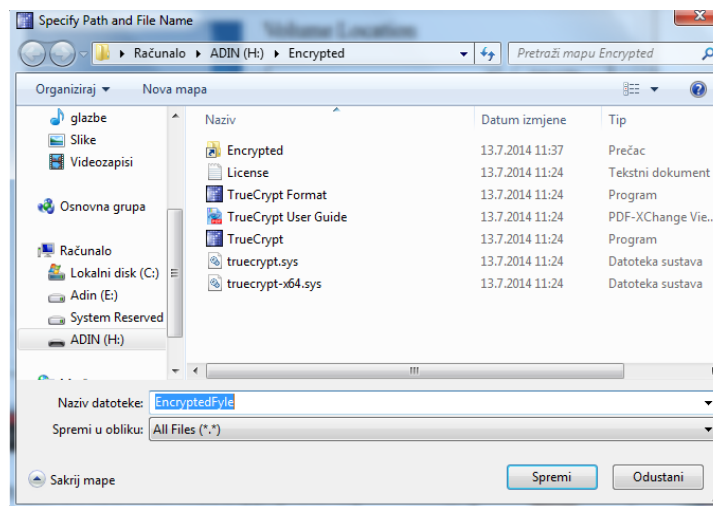


Picture 19 Create Volume

Now we need to create an encrypted Container and tell the program where we want to save the Container. This file will contain all we want to lock.

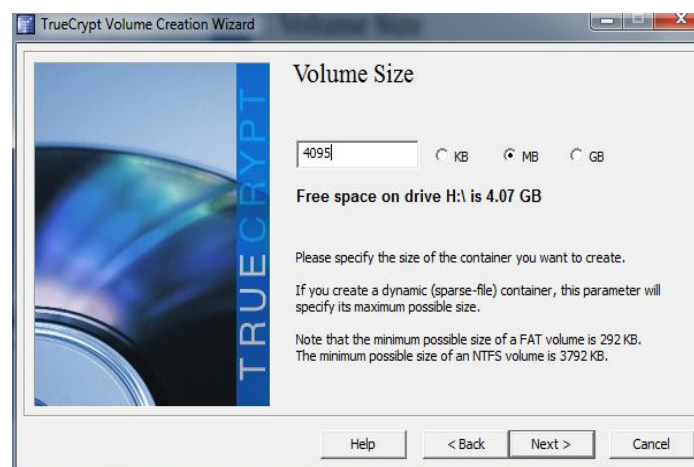


Picture 20 TrueCrypt Volume Creation Wizard



Picture 21 Specify Path and File Name

The next step is the size of the container and its max value is 4096 MB. Enter the size of the container.

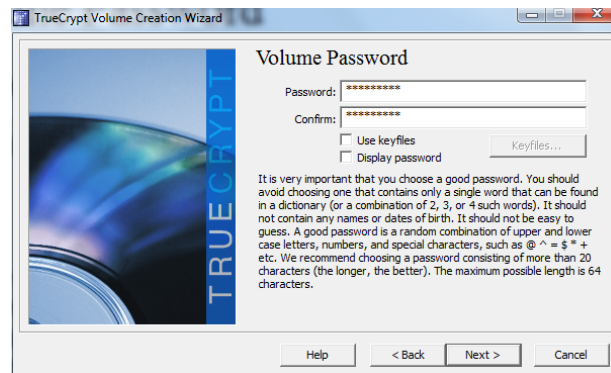


Picture 22 Volume size

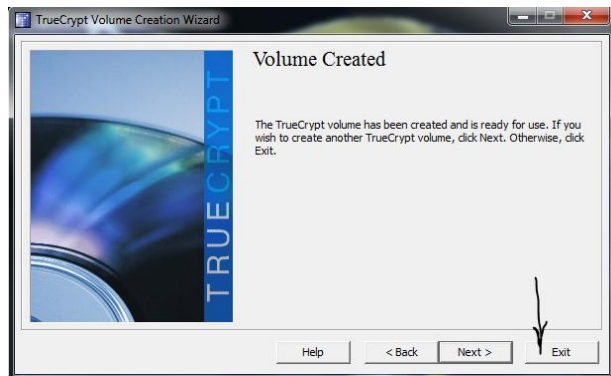


After the 'Next' you need to create a password.

RECOMMENDATION: Some code that is long and which needs to contain special characters ('= &% \$ #).

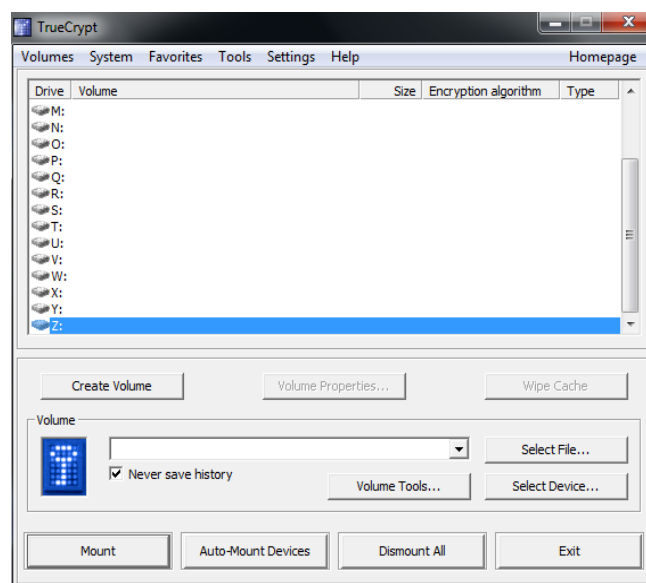


*Picture 23 Volume password*

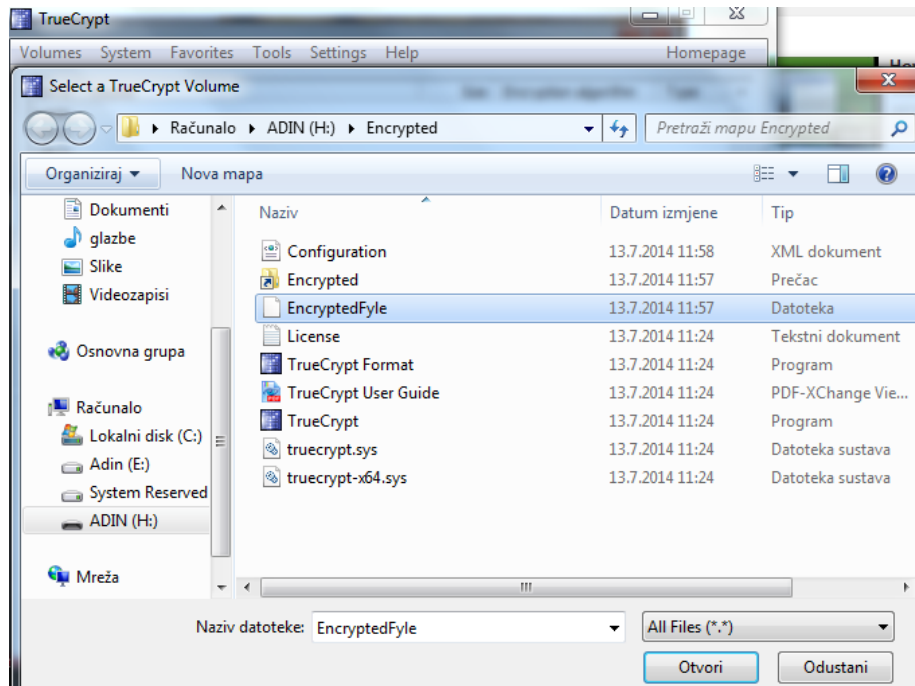


*Picture 24 Volume is created*

Then click on the letter of the virtual drive and choose Select file. Find encrypted Container that we made at the beginning and click Open. Then click Mount, type in the password and click OK.



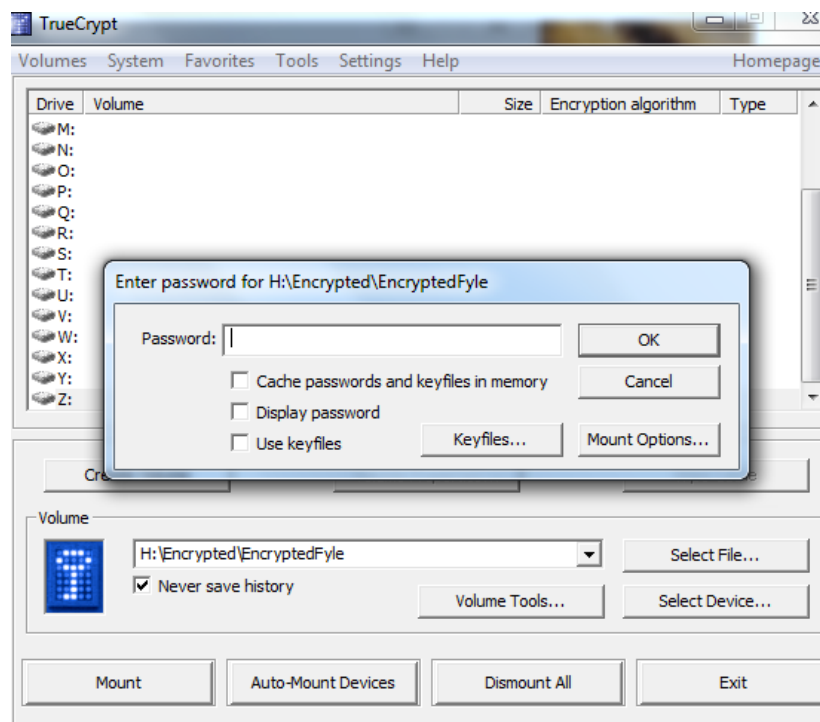
*Picture 25 Opening a file*



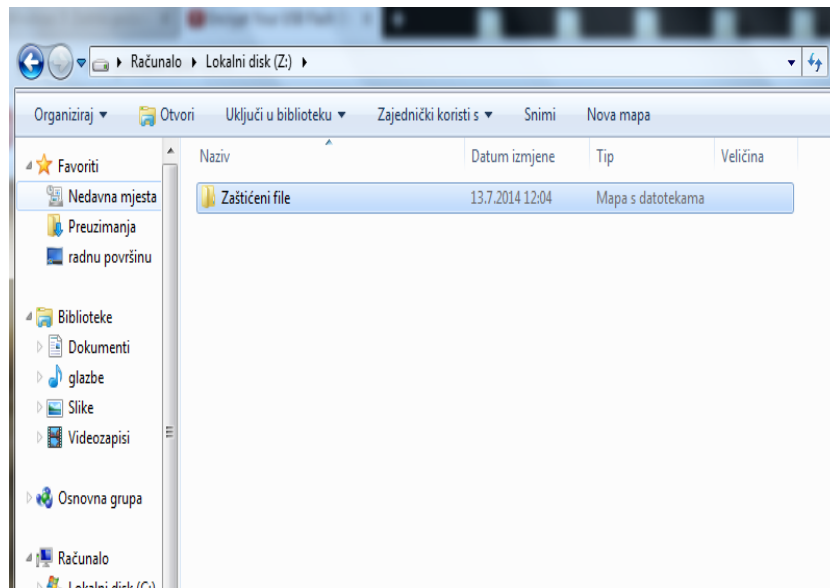
Picture 26 Steps for opening

Now we have on file My Computer new disc in which we can put large files. When SMOS team finished, restart the program.

From now on, when we want to access a data we run the program and find containers. Then we put them under a certain letter and then mount the disk. You need to type in a password and access the data.



Picture 27 Mount the encrypted file



*Picture 28 Protected file*

#### **4 CONCLUSION**

USB memory stick is something that most of us use every day. This medium is used for private purposes as well as for business purposes. Often, this media is not getting enough attention from us even though we are at it stored important information. Therefore, we are in danger of unauthorized access or data theft.

TrueCrypt is an open source application that can protect data, in this case with a USB memory stick. After extractions program on a stick and explained the procedure, protected data with stick approach on any computer mounting the drive with a predetermined input our password. This is a very useful application and its main asset is that it is free.

## SALES OF PHOTOGRAPHS

Bajro Ljubunčić<sup>1</sup>, Amra Mirojević<sup>2</sup>, Almira Salkić<sup>3</sup> and Emir Brčanić<sup>4</sup>

UNIVERSITY OF "VITEZ" VITEZ

Bajro.ljubuncic@unvi.edu.ba, amra.mirojevic@unvi.edu.ba, almira.salkic@unvi.edu.ba,  
emir.brcaninovic@unvi.edu.ba

### SUMMARY

*The development of modern means of communication plays a significant role in the globalization process, because they are changing existing relations in the global market. The impact of ICT has spread to the activities in which previously there was no possibility of their application. Graduating from mechanical to electronic phase of trade leads to faster penetration of technical processes. Or come up with the development of electronic stores (Web shop) which have many advantages but also its disadvantages.*

*The problems are primarily reflected through the methods of payment and security of Internet transactions. Notwithstanding this volume of retail transactions carried out through the Internet are increasing. Business users who want to develop e-commerce and enter into the kind of system operations usually turn to companies that they will all need to make and deliver. In recent years, appearing tools that enable IT less literate customers to do the job of programming through wizards. Internet business provides an opportunity to improve your way of working thanks to the global availability of the Internet. It supports all the ways of doing business through the internet i.e. buying and selling of goods and services, performing financial transactions electronically, promotion and marketing activities and others. Shop online increases the profitability of the company through its ease of use and reduced cost.*

**Keywords:** Internet, trade, e-commerce, applications, e-business

### 1. INTRODUCTION

With the development of ICT technologies (ICT) in their entirety are changing many affairs. Work of computers aims at facilitating the work of its customers in all areas of life and business. Technology is an additional tool that allows efficient implementation of activities. In modern business there is a transition from mechanical to electronic way of doing business, which implies faster penetration of technical processes in commerce. The development of electronic shops aims to facilitate the purchase of products from anywhere on Earth. Computer technology is automating sales in traditional retail establishments (shops, salons, department stores) enabled the centralization of supply management, production, pricing, distribution, sale of goods, stocks with a view to more efficient and effective and profitable business.

Issues that trigger making this paper are: What e-commerce?, How it works?, What are the advantages and disadvantages of e-commerce?, How to make e-commerce? The subject of this research is based on the research literature to determine how to program a web shop to sell

photos. The primary purpose of making this work is complete and comprehensive introduction to the field of electronic commerce, its operation and implementation of the sale of photographs. Therefore, the goal of this research is to investigate, identify and interpret web shop to sell photos.

Internet is a daily basis part of business because it offers the opportunity for advancement. E-commerce represents all ways of doing business that has been done in a traditional market: buying and selling of products and services, financial transactions electronically, promotion and marketing Execute a et al. It is one of the more profitable forms of trafficking, as simplicity, low cost, and lack of working time are part of the benefits that this trade provides.

According to the report, of e-commerce there are 618 million potential customers. Retailers do not pay business rates but they need just one web site the the product is available to everybody. According to the same report of 816 million, 565 million users as Internet users, while 264 million are Internet customers. The advantage of this trade is reflected in the fact that there are no geographical limitations, but the product is available to most remote users.

## ***2. DETAILS OF MAKING WEB PAGES***

Internet market is one of the largest emerging markets. Users can decide to this type shopping because it implies more choices, and then compare prices between multiple vendors and delivery to the door, which for them is a time-saving. All information can be immediately updated and so the information before coming to customers. Virtual stores offer a large number of products and the role shall. From the organization's services and the provision of travel, shopping for shoes or clothes, beauty products and health books and literature, to basic household necessities.

In the planning of e-commerce is necessary to achieve a few basic steps. First of all: making a decision and timing of establishing a virtual store, the selection of assortment of products and services, the choice of payment method in the virtual store and distribution organization products, domain registration and opening Web site (server support), creating a website for a virtual shop, a maintenance plan and promotion of virtual stores.

The first and basic step is that top management makes a decision about establishing e-commerce. The decision is based on the analysis, reflection goals that should be achieved with e-commerce. Establishment of e-commerce is reduced to opening the website, choice assortment of products and services, selecting payment. When choosing a web address it is necessary to strive that her name be informative, unambiguous, attractive and original.

Web site creation and implementation of the trade is an important process and it is necessary to engaging an experienced team of professionals who will follow all necessary steps to bring the product documentation and work on further maintenance and technical support. When the creation process is complete, it is necessary to carry out to promote and ensure the marketing mix that will ensure the attendance of trade, and lead ultimately to the desired volume of sales and profits.

The advantages of e-commerce are: market size, the ability to purchase products where he is the cheapest, reduce operating costs, fast and cheap realization of orders, saving time, flexibility in business, increase business efficiency. The disadvantages are: necessity, constant investment in further development, the difficulty in finding employees with appropriate experience, the risk of fraud, the marketing costs associated with the tough competition, identity theft customers.

To make a successful e-commerce we must comply with the basic requirements which keep users on websites, such as: easy to use, easy to navigate, the products split into categories, size of assortment, information, security, and process shopping, marketing on the site, design, motivation and words. Website we need to make it simple because complicated e-commerce discourages users from buying, they cannot manage and canceling purchases of buying. When the user easily handles the page it simply will reach your goals i.e. purchase.

Products and services should be divided into meaningful categories and subcategories. It is necessary to produce updated frequently and provide summaries of the product to enable more information. Too large range of services or products may cause customer confusion, it may confuse him. So be aware of the size range. When a user comes to the site is necessary for us to give him all the information about the product or service, such as product information, technical specifications, instructions for use, potential services, complaints, returns, instructions on maintenance and more. Web shop is specific for security because it is essential that the user leaves no doubt that does not ask questions about whether the product terminal rank or whether it can be returned in case it does not work flawlessly. ☒

To satisfy their desires, it is necessary to provide them security of data transfer, a statement of non-operation of personal information and other information about the contact with the company. Questionnaires and other marketing activities, it is necessary to leave at the end or optional for shopping in order to avoid further bother the customers.

Advertising and other forms of promotion should be made discreet. Page design we adapted to the product for which we specialize, and customers who are our target group. It is necessary to motivate users to return to the page after a successful purchase. We put related products or encourage the reduction or other actions that are specific to our company and thus motivate him to further purchases. When writing text content we should be careful to be specific information, specifications, recommendations, and not empty promises.

In the electronic shopping safety was a major disadvantage that provided confidence in her. Then there were no sufficiently developed systems to encrypt and protect customers. Web shop should provide a sense of security, the buyer should not have the fear that you will receive the product or not, we need to believe that he can entrust us with their personal information and money. For this we use SSL protocols that allow safe to send different data without being able to read the same data by other persons. It is a system of encryption that uses a large amount of data that is impossible to decipher in the short term. Therefore is used to send credit card numbers and other sensitive data.

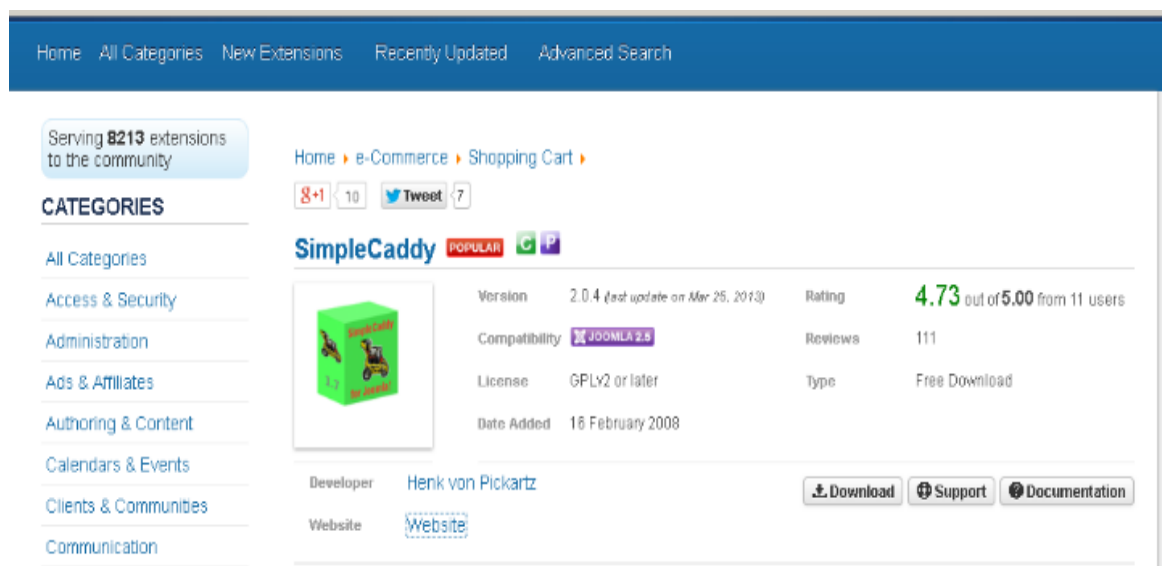
One way of checking the website is an inscription in browsers (https) which indicates that the vendor uses a secure server to receive data. Digital certificates and digital signatures are an asset that provides additional security when purchasing products. These certificates for companies providing international companies that are exclusively specialized in the issue of such certificates. It is impossible to make a web store that will accept credit cards as payment without

such certification. E-commerce offers the possibility of sending you a check by each bank, and the money we send a special fast banking system.

### 3. THE NECESSARY RESOURCES

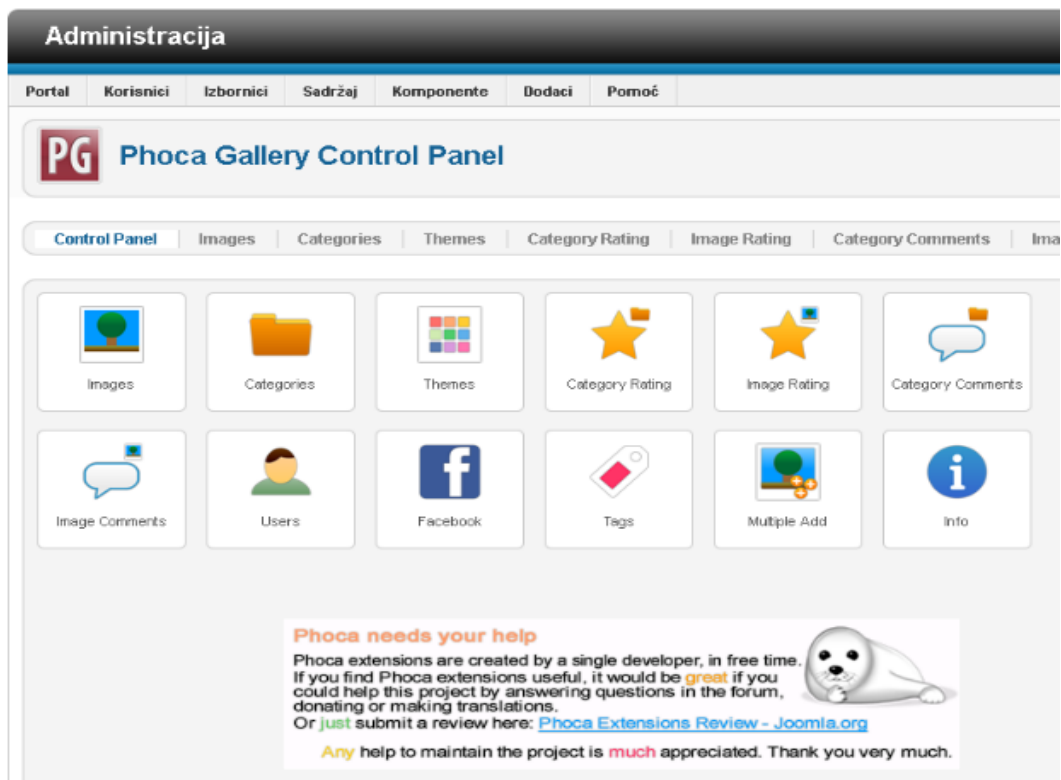
We used the Joomla CMS and its components Phoca Gallery and SimpleCaddy.

Joomla is an award-winning content management system (CMS), which enables you to build Web sites and powerful online applications. Many aspects, including its ease-of-use and extensibility, have made Joomla the most popular Web site software available. Best of all, Joomla is an open source solution that is freely available to everyone.

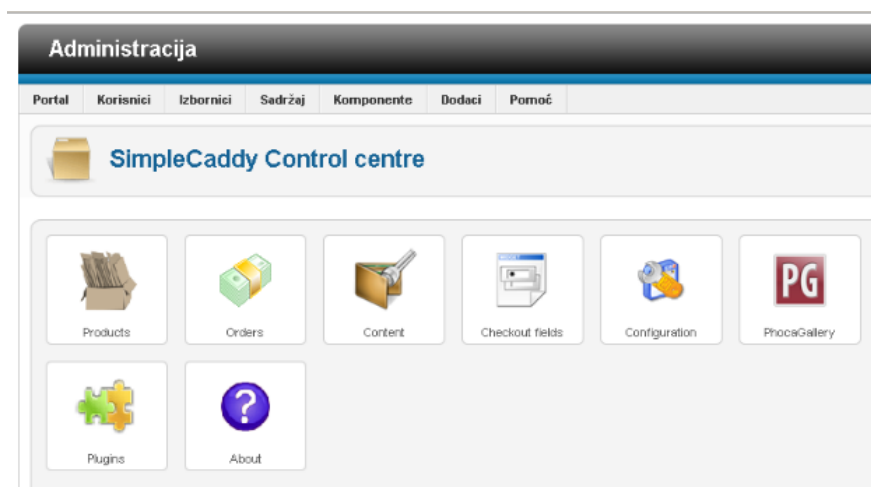


*Picture 29 Page layout of Joomla*

A content management system is software that keeps track of every piece of content on your Web site; much like your local public library keeps track of books and stores them. Content can be simple text, photos, music, video, documents, or just about anything you can think of. A major advantage of using a CMS is that it requires almost no technical skill or knowledge to manage. Since the CMS manages all your content, you don't have to.



Picture 30 Phoca Gallery Control Panel



Picture 31 SimpleCaddy Control Centre

Joomla is used all over the world to power Web sites of all shapes and sizes. For example:

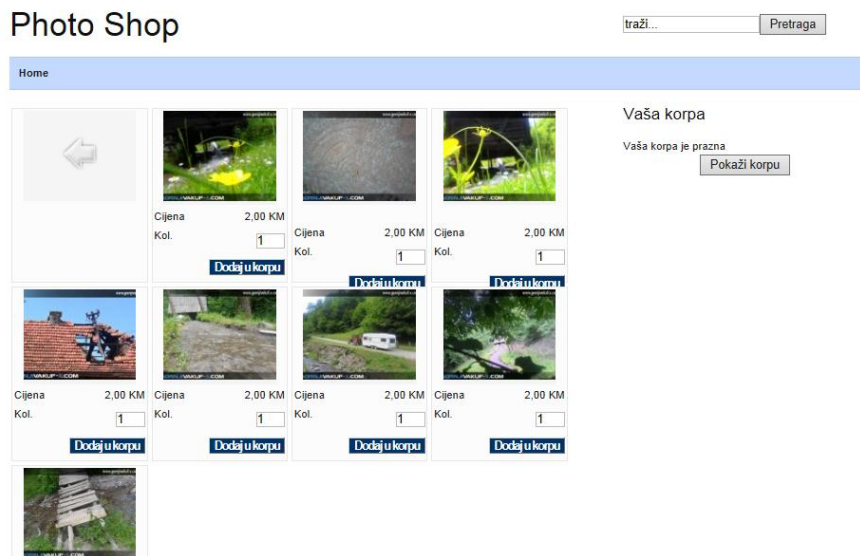
- Corporate Web sites or portals
- Corporate intranets and extranets
- Online magazines, newspapers, and publications
- E-commerce and online reservations
- Government applications
- Small business Web sites
- Non-profit and organizational Web sites



- Community-based portals
- School and church Web sites
- Personal or family homepages.

#### 4. THE WEB SITE PAGE LAYOUT

Respecting the principle of simplicity and ease of use our website has this look.



Picture 32 Page layout of website

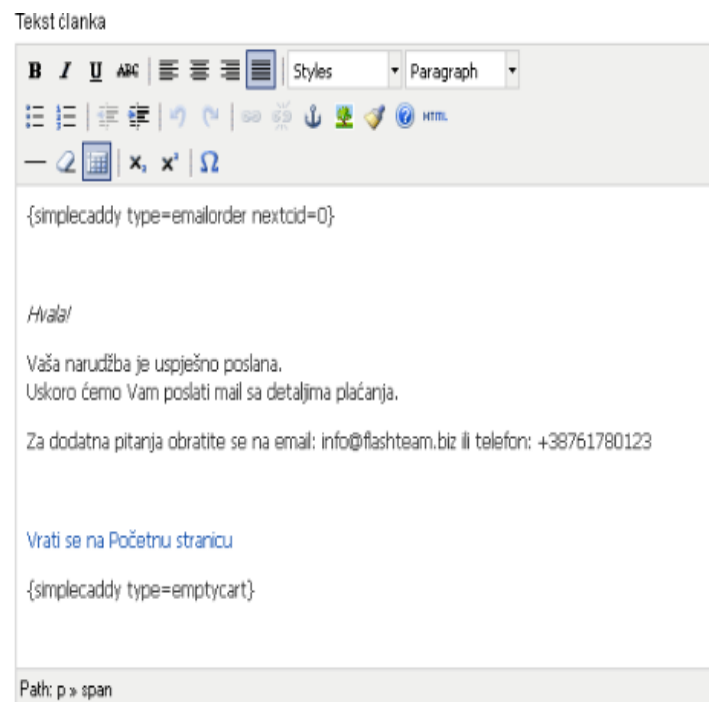
After the selection of photos, they are put in the basket. Order form to fill up your personal data and executes it.

Picture 33 Ordering process

If the customer completes a purchase, at inbox comes an email with the order, and the user receives a message that the purchase has been completed.



*Picture 34 Order confirmation on website*



*Picture 35 Order confirmation for costumer with email*

Narudžba od Bajro Ljubuncic u iznosu od 8,00				
Pristigla pošta x FLASHteam x				
Photo Shop				
prima bajro.ljubuncic				
Naruči				
11.07.14				
Bajro Ljubuncic				
bajro.ljubuncic@gmail.com				
Neka ulica 33				
70240				
BiH				
061 111 222				
24				
Kod	Naziv	Cijena	Kol.	Ukupno
skljoc	Skljoc - - ewrwer.jpg	2,00	4	8,00
		Ukupno		8,00

Picture 36 Email with order

## 5. CONCLUSION

E-commerce is one of the more profitable forms of trafficking, as simplicity, low cost, and lack of working time are part of the benefits that this trade provides. According to the report, of e-commerce there are 618 million potential customers. Retailers do not pay business rates but they need just one web site the product is available to everybody. According to the same report of 816 million, 565 million users as Internet users, while 264 million are Internet customers. The advantage of this trade is reflected in the fact that there are no geographical limitations, but the product is available to most remote users.

It offers us many opportunities to make a web page using proven software and with little knowledge of programming. All the resources that are available to us, we need to use it. An application with open source code has its advantages and disadvantages that we should be careful in the planning phase of developing the site.

## 6. REFERENCES

[1] Joomla

<http://www.joomla.org/about-joomla.html> (20.07.2014).

[2] Models

<http://www.shop.hr/category/moduli/> (20.07.2014)

[3] B2C Commerce report for Europe 2014.

<http://www.ecommerce-europe.eu/home> (20.07.2014)

[4] Internet commerce is growing 10 times faster than classical

[5]<http://marker.hr/blog/internet-trgovina-putem-smartphonea-i-tableta-u-strelovitom-rastu-145/> (20.07.2014)

# BUSINESS INTELLIGENCE

Grabus Elvis  
UNIVERSITY OF "VITEZ" VITEZ  
elvis.grabus@unvi.edu.ba

## ABSTRACT

*Business intelligence includes the processes, technologies and tools that help in transforming data into information's, information's into knowledge and knowledge into plans for management of the organization.*

**Keywords:** *business intelligence, BI, OLAP, Data Mining.*

## 1. INTRODUCTION

Business Intelligence (BI) systems help: testing and analysis (ad-hoc reporting, analysis tools), reporting (dashboards, trend analysis) to plan, budget and forecast (plan - achieved) performance management (indicators). These systems provide a unique access to information's, response to business issues, and the use of BI systems throughout the organization. The main limitations of BI software are high cost and long period of implementation of such system. An important concept related to the application of the business intelligence software is a Data Mining (mining). Data mining can be defined as finding regularities in data. The areas in which Data Mining can be successfully applied are varied, for example, the company's operations, economics, mechanics, medicine, and genetics and so on. Any organization that deals with the production function, and profit as the ultimate goal, is actually a dynamic system, which is characterized by its current state and the state in which the system can move to the future. These states are represented by a large amount of data, which is recorded in various types of information systems, document and other sources of information. The processing of these data, find the causes all relationship (correlation) between them and their transformation into information is a significant potential for growth. Information is a key factor in decision-making at any level of operating through the middle to the strategic level of decision making. Therefore, their proper interpretation and generate significantly influence the choice of model management actions, which will use the company's management. Electronic mode of operation becomes inevitable and dominant compared to current methods of doing business (slower and less efficient), and the main performance indicators (efficiency, effectiveness, productivity, and profitability), are directly related to the quality and degree of implementation of information technologies used for this purpose. Information technology infrastructure is the basis for the process in a modern business system. Business Intelligence Business Intelligence (BI) is part of the information system of organization that is dedicated developed to enable performance management organization. Business intelligence is an area in the field of information technology, which aims to overall enterprise information resources put to use making the best decisions to achieve the strategic goals established companies. It is a very complex area that includes various types of technologies and approaches in the field of information technology,

management, statistics and mathematics. The basic question that comes to mind when talking about this yet innovative software solutions in the world of modern business is “Do you use a business intelligence system or not?”.

## **2. WHAT IS BUSINESS INTELLIGENCE?**

In order to know what is actually a business intelligence or business intelligence, first we must define the term in order to know in what way, in which case use the term and what is actually meant by Business Intelligence. Business Intelligence as a discipline designed in the seventies of the twentieth century, and one of the many definitions as follows: “Business Intelligence (BI) is use the collective knowledge of the organization, in order to achieve a competitive advantage”. Business intelligence includes the processes, technologies and tools that help in transforming data into information, information into knowledge and knowledge into plans for management of the organization. The term Business Intelligence (Business Intelligence, BI) combines methodologies, technologies and platforms for data storage (Data Warehousing), network analytical processing (OLAP Online Analytical Processing) and Data Mining that enable enterprise organizations to create useful management information from the data on the operations that are dispersed in different transaction systems and come from a variety of internal and external sources. Such information is presented for the efficient use of strategic and tactical and operational audits and making decisions. Based on this it can be concluded that the business intelligence actually a technique that lets you find the information needed to make it easier, faster and more accurate decision making. Business intelligence is created or evolved from a decision support system used in the U.S. companies 60s of the 20th century. The concept of Business Intelligence in the Serbian language translates as business intelligence. But, in the English language the word intelligence has two meanings: the ability to learn, understand, logical thinking, an ability to do things well; secret information collected about a foreign country, especially a hostile, people collecting the information. The basis for understanding the concept of BI are three items (principles):

- Ethical process of gathering information, which, after appropriate processing becomes knowledge;
- The focus on information that is planning future events; and
- Instrument that has a full role in the decision-making process.

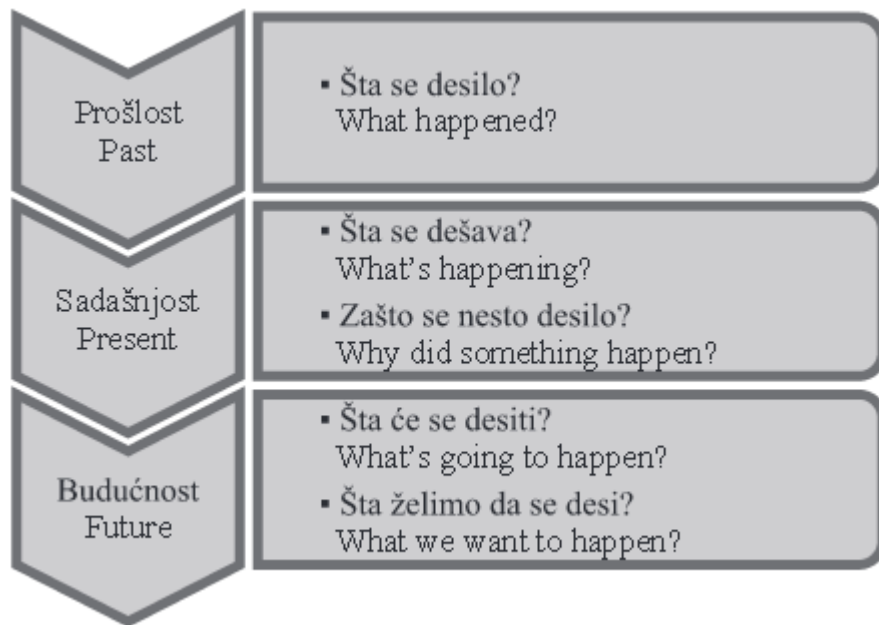
## **3. WHY BUSINESS INTELLIGENCE?**

One of the main questions that are often asked by the organization itself and its management is exactly why we needed and what will promote the introduction of these, we note, no cheap system. The main reasons for the introduction of business intelligence systems are as follows:

- Environment is no longer static. Offered products and services are huge, the competition is high. Research shows that present supply of goods and services at least 30% exceeds demand (markets are saturated). New circumstances require new solutions, new challenges of the new effort. Just production of goods and services is now a past.
- Globalization of markets, the development of distribution channels, “interference” in the internet business, things have changed. Now the buyer and seller are at the distance

of a click of the mouse. Today, the company is overloaded with data. On the other hand, there is a lack of useful information. To minimize the gap between the amount of available data and information necessary to define the processes of data collection and their “processing” in the information. The response time to the environment should be reduced, preferably to real time.

- Resources are always limited. Time as the most important factor is almost always essential. Therefore, you should know where to set the lever to move a large rock. How to act in order with a minimum of fuss resolve most problems?
- Decomposition of the value chain (procurement, storage, production, sales, after-sales activities) to the proper use of a lever effect. In addition, it allows us to find fundamental solutions to existing problems, not the symptom. Usually the effect is greatest leverage in sales.
- Finding new customers is ten times more expensive than retaining existing ones. If the company fails to reduce the exodus of buyers competing for 5%, it is very likely that this may double their earnings.
- A great danger threatens the enterprise of hidden customer dissatisfaction. Only 4% of dissatisfied customers complain about the poor quality of products or services. 90% of customers, who are not satisfied with the quality of the product, will avoid the product. Each of dissatisfied customers will inform the other ten to twenty people.
- Customers are leaving because they are unhappy, though they never complained. A buyer who leaves a company, it cannot return.
- Customers (with employees and their knowledge) are the largest value that the company owns. How to keep them? Stable relationships with customers are the key to long-term success of the company.
- Maintenance of operational liquidity management is the problem. Solutions to this problem directly affect performance of management. In order to master these operational problems, company should be familiar with their customers, suppliers, processes, and connections between them.
- To keep the cycle Operating Controlling (data collection, planning, analysis and control, and management) in the company to work, to have the information infrastructure.



**Picture 1:** Why should we use BI system?

BI systems help to:

- Testing and analysis (ad-hoc reporting, analysis tools);
- Reporting (dashboards, trend analysis);
- Preparation of plans, budgets and forecasts (plan - achieved); and
- Performance management (indicators).

BI enables organizations to system actually promote cultural understanding and taking action through:

- Making decisions based on facts;
- The quality of information;
- Coherence forms of information;
- The quantity of information; and
- Sharing of information

#### **4. WHO USES BI SYSTEM**

BI system was originally designed for decision makers and the people who make business decisions. Today, corporate decisions are made by everyone. Not all decisions, but all we can suggest. It's not a return to the self-management, but to provide opportunities for all those who can contribute to the preservation of the vitality of enterprises. Information and knowledge are needed by everyone.

#### **5. COMPONENTS OF A BUSINESS INTELLIGENCE SYSTEM**

There are several different types of the components that, in general, are not too important in the basic definition and understanding of business intelligence. The only division that at this level is important to basic includes:

- infrastructure database for data warehousing, ETL tools (used to collect data from multiple sources, regardless of the technological solutions), the operational data storage;
- functionality Data Mining (treated separately below), BI platforms, applications (operational, strategic and analytical), ad- hoc reporting;
- organization performance Measurement, Information/corporate culture, BI methodology, centralized BI (integration of knowledge and skills);
- management the key indicators of the performance of external transparency, trends.

## 6. DEVELOPMENT OF A BUSINESS INTELLIGENCE SYSTEM

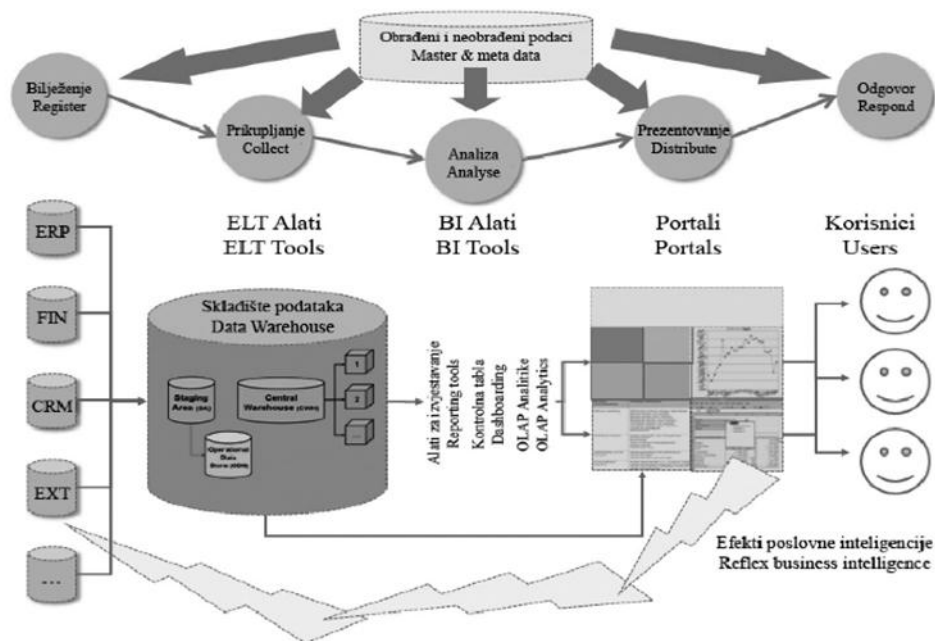
Intensive development of BI is directly linked to the period when the company began to automate their business processes through the implementation of various systems, and thus create the possibility of generating large amounts of data. There has been an explosion of data, which is reflected in the exponential growth of their quantity. Increased the number of bases that have placed the data, but automatism search did not exist or were very underdeveloped. Practically, they possessed a large amount of data that were unusable because they were difficult to access. In parallel, there was the awareness that these data can be very useful in the hands of management. Management, however, does not work with data, but the information and how the information = data analyzed, it is clear that the aim was to develop a system that will process the data. Based on the data presented by Nigel Pendse (2008) can see the development of the BI market over a period of 14 years, and forecasts of its growth, which can be seen as gradually in the period since 1994th until 2007th. The rising value of the BI market, expressed in billions of dollars, with a value of \$ 0.5 billion (which was the market value in 1994.), up to 5.5 billion U.S. dollars (which was the value of this market 2007 year:

Godina Year	Vrijednost u milijardama \$ Value in billions \$
1994.	0,5
1996.	0,95
1998.	2,05
2000.	3
2001.	3,3
2002.	3,5
2003.	3,7
2004.	4,3
2005.	4,8
2006.	5,5
2007.	6,4
2008.	6,9

**Table 1:** The growth of OLAP market Source

The most important thing is to emphasize that in this system, respectively, it should be noted content management systems, ETL tools, BI tools, analytical systems and users (managers) at the end.





**Picture 2:** BI infrastructure

Main features of Business Intelligence (Business Intelligence) are the following:

- unified access to information;
- answers to business questions, at the time and
- The use of BI systems throughout the in every part of organization.

These are the three basic characteristics of the system, which is also referred to as the three primary advantages of introduction and implementation of this system in the business process brings. As the primary advantages of using systems Business Intelligence, provides the following characteristics of the system:

- improve operational efficiency;
- the elimination of the backlog of reports and delays;
- finding the cause of the problem and take measures accordingly;
- better communication with customers and suppliers;
- identification of "waste of resources" and reducing inventory costs;
- sales information to customers, partners and suppliers;
- improving strategies with better marketing analysis;
- gives users the means to make better decisions;
- dealing assumptions with facts. (Dropped item which said Take your investment in ERP or data warehouse).

The main disadvantages and we can say restrictions that accompany such systems, like business intelligence systems are:

- the high cost of software;
- expensive and long time training to use;
- requires a large range of experts in the field of technology;
- mixing data from different sources;
- send requests to retrieve data from business intelligence systems can be tedious and time-consuming, with aspect of the system users.

## 7. IMPLEMENTATIONS AND APPLICATIONS

The introduction of BI systems is a process which is practically endless. At the time of the unstable environment that is becoming hyper aggressive, and therefore an uncertain future, business intelligence must constantly evolve as requirements analysis and forecasts become more complex, especially when added to the need for high speed processing and performance (real-time as a key notion of information now). Raises the question for us is the price of such systems and cost information. In the 21 Ages, Ages of information and knowledge, price of information is equal to the price of survival in the market. Establishment of a system for management of business information is a profitable investment. Accounting does not record opportunity costs of bad business decisions based on lack of information. Such failures are recorded stock market and competition. These two “gauges” unmistakably know penalize weaknesses of business. BI system does not exist as a finished product; there are manufacturers that offer technology platforms and knowledge to implement. There are no off the shelf solutions. The reason for this is the fact that the decision models are similar, but the strategy, market segmentation and product, processes and relationships between them are different. Are also heterogeneous data sources that “food” these systems. Big manufacturers are roughly divided into two groups of databases - IBM, Oracle and Microsoft - whose bases are used as a basis for building a data warehouse. That platform they use as a base. Clients also offer front-end tools for end users, implementation and business models. Original manufacturers, and from which need to allocate the four great that have a significant presence on the regional market - SAS, Cognos, Business Objects and Micro Strategy. Their main focus is the front-end tools for end users that can be connected to any of the platforms for the database. They are, except for the SAS which is present with subsidiaries in the countries of our region, present through authorized distributors. Many large and medium-sized companies active approach to the notion of business intelligence, development and implementation of these systems and use them in your e-business. Companies thrive to turn information into business intelligence, business intelligence in corporate knowledge and collective knowledge to increase profits. According to the previous description, can be specified several areas in which suitable application of business intelligence:

- Reduction in operating costs, the realization of sales targets, improving the procurement system
- Using OLAP (On-Line Analytical Processing) to reduce the cost of IT sector, discover new opportunities for profit improvement cost management;
- Using Data Mining to find the key parameters related to a specific customer segment.

All these applications are only possible with the use of sophisticated tools and applications, if the data are prepared in a format suitable for various types of analysis. For business users it is important to have the tools and applications you will be able to analyze the data, and the IT people important to have the applications and tools to create and manage the environment for business intelligence. For this purpose, various tools such as:

- dedicated applications;
- tools for querying;
- OLAP tools;
- tools for statistical analysis;
- tools for Data Mining and others.

## 8. CONCLUSION

Business intelligence system is a system that stores information and knowledge on competition, customers, suppliers, processes. It allows business negotiation and reasoned approach to numerically customers and suppliers, quality operational planning, monitoring the behavior of competitors, the observation of individual market segments and predict future events. Also, the business intelligence system provides a better understanding of their own customers and realizes that encourages them to certain behavior. On the technical side, business intelligence is the process by which raw data is converted into information. This information is then analyzed and used in the decision-making process in the company. No demur - the answer is definitely "To BI." Business Intelligence ( BI) systems have become an indispensable tool for all levels management in decision-making processes. The concept of business intelligence in the last few years is so current that it is almost impossible to avoid, which is not surprising, since it offers a solution to one of the biggest problems of management – making good business decisions.

## 9. LITERATURE

- [1] Ćirić, B., „*Business Intelligence*” Beograd, 2006
- [2] Javorović, B., Bilandžić, M., „*Business information and business intelligence*“, Golden marketing Zagreb, 2007
- [3] Krulj, D., „*Projecting and implementation Data Warehouse and Data Mining systems*“, Golden marketing Zagreb, 2007
- [4] Panian, Ž., Klepac, G., „*Business Intelligence*“ Masmedia Zagreb, 2011
- [5] Paul, S., Mac Lennan, J., Tang, Z., „*Data Mining Tutorial*“, Microsoft Corporation, 2005
- [6] What is Business Intelligence (BI)?  
[http:// www.passionned.com/business-intelligence/what-is-business-intelligence-bi/](http://www.passionned.com/business-intelligence/what-is-business-intelligence-bi/)  
(23.08.2013)

# DATA ENCRYPTION

Benjamin Destanović<sup>1</sup>, Senida Kakeš<sup>2</sup>, Hasmir Musić<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

benjamin.destanovic@unvi.edu.ba, senida.kakes@unvi.edu.ba, hasmir.music@unvi.edu.ba

## ABSTRACT

*Today, data encryption is most widely used method of protection of data and information that contains confidential information. There is a number of methods available for use to achieve specific degree of data protection, depending on required level of protection. In last few years, methods and implementation protocols of data encryption have changed leading to weakening of efficiency of such methods. Today, the main cause of security problems associated with traditional methods come with the fact that today's computers are more advanced than ever.*

**Key words:** *Cryptography, encryption, data protection, quantum cryptography*

## 1. INTRODUCTION

Data encryption is a process in cryptography which protects the data so that the message or information is unreadable for people who do not possess a certain knowledge (key). This term is used in computer science, where certain data packets and informations are encrypted and sent from one location to another through a medium such as Internet. In the scheme of encryption, message or information is encrypted by using one or more of the available methods of encryption, transforming message thus making it unreadable for a party that is trying to steal it. This is usually done by using the encryption key that determines the way of encoding the message. Any unauthorized party who can see the encrypted message must not be able to determine anything about the original message. The authorized parties should be able to decode encrypted message using decipher algorithms of which some of them usually require decryption key that unauthorized parties do not have.

## 2. ENCRYPTION METHODS

There are two basic types of encryption schemes: scheme of private-key encryption and scheme of public-key encryption. Private key encryption scheme uses the same key to encrypt and decrypt the data and information. This means that parties communicating while using private key scheme must agree on a secret key to be used before establishing communication. In contrast, in scheme with public key encryption everyone has the access to the key for encryption, and can encrypt messages. However, only authorized parties have the key required to decrypt the message.

## ***2.1 Private key encryption***

When using encryption with the private key, each computer has a secret key (code) that can be used to encrypt packets of information before they are sent over the network to another computer. This method requires knowledge of computers that will communicate, so the key can be set to each of them.. This encryption method is based on the fact that both computers know the decryption key that can be used decipher and exchange messages. The first major algorithm for generating symmetric keys for computers, Data Encryption Standard (DES), was developed in the United States, and was approved for use in 1970. The DES uses a 56-bit key. Although 56-bit key can generate over 70,000,000,000,000,000 combinations, appearance of advanced computers sought the need for better algorithm and DES was replaced with Advanced Encryption Standard (AES) algorithm. AES can use 128-, 192- il 256-bit keys to generate private key. Private key algorithms are the algorithms used for cryptography that use the same cryptographic keys for encryption and decryption of clean data. The keys may be identical or may differ only by small bits between the decryption key and encryption key. In practice, the keys are "shared secret" between two or more parties wanting to establish secure communications, which requires that all parties participating in the communication must know the secret key. This is the main disadvantage of this private key encryption method compared to the public-key encryption.

## ***2.2 Public key encryption***

Public key encryption uses two different keys at once - a combination of a private key and a public key. The private key is known only to the computer commencing the communication while the public key is given to any computer that wishes to establish the communication. To decode the encrypted message, a computer must use the public key, provided that the key was previously given to him by a computer that commenced the communication. Although the message sent from one computer to another will not be safe because the public key used to encrypt is published and available to everyone, not everyone will be able to decipher the message without the private key. Generating a key is based on prime numbers (numbers that are evenly divisible only by itself and number 1, such as 2, 3, 5, 7, 11 and so on). This means that this encryption scheme is very secure, because there is essentially an infinite number of primes available for key generation meaning there are almost endless possibilities for key combinations. One very popular program for data encryption using public-key method is Pretty Good Privacy (PGP), which allows data encryption using public key. This type of encryption is considered very safe since it does not require sharing any secrets between sender and receiver. Very popular implementation of public key encryption is the Secure Sockets Layer (SSL). Originally developed by Netscape, SSL is a protocol for Internet security using Internet browsers and Web servers to transmit sensitive information. SSL has become the protocol of general security for transmission of sensitive information known as Transport Layer Security (TLS). In your browser you can see when a secure protocol is used such as TLS in several different ways. You will notice that the "http" in the address line will be replaced by "https", and you should see a small padlock in the status bar at the bottom of your browser window. When accessing sensitive information, such as online bank account or payment services for the

transfer, such as PayPal or Google Checkout, it is required to use this protocol because of information safety.



**Image 1.a:** HTTPS in the address line indicates the use of security protocol



**Image 1.b:** Padlock in the status bar indicates the use of security protocol

When a browser requests the use of protocols for safety, it adds "S" to "http" and the browser sends the public key and the certificate, checking for three things:

- 1.) That confirmation comes from a trusted party
- 2.) That the certificate is currently valid
- 3.) That the certificate has a relationship with the source it comes from.

Encryption key used in the public key encryption is based on the hash values. This is a value that is calculated from a base using a hashing algorithm. In essence, the hash value is a summary of the original value. What makes the hash code so reliable is the fact that it is almost impossible to know what is the value of base input without knowing the method used to generate hash code, for example:

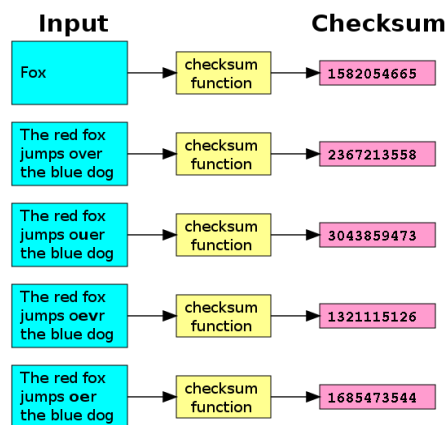
**Table 1:** Hash algorithm

BASE	Hash algoritam	Hash value
10,667	Base x 143	1,525,381

In this example, the hash value is 1,525,381, and there is no possibility to know what is the original value (base number) if method used to generate the hash code is unknown which in this case is generated by multiplying the base with nubmer 143.

### 2.3 Cheksum functions

Another requirement of secure-computing is to ensure that data is not damaged during transmission or encryption. There are several popular ways to do this. Probably one of the oldest methods of ensuring that the data is accurate is the checksum method which provides a test of accuracy of the data because an invalid checksum suggests that the data has been corrupted during transmission or encryption. The process which generates a checksum is called a checksum function or checksum algorithm. Checksum functions are associated with the hash functions, functions that operate on the principle of fingerprints, randomization functions, and cryptographic functions. However, each of these concepts has different applications and therefore different goals. It is important to mention that one should not use the checksum in safety-related applications because checksum does not have the properties to provide data protection in case of intentional attacks.



**Image 2:** Cheksum function example (with cksum utlitiy application)

### 2.3 Cyclic redundancy check

Another way of checking the data accuracy is the method of the Cyclic Redundancy Check. It is very accurate method of detecting errors that are commonly found in digital networks and storage devices caused by accidental changes in the original data. The blocks of data included in this scheme receive an attachment of short confirmation value based on the remains of the polynomial division of original content. When returning the data value, the value is read again and corrective measures can be undertaken if the value does not match with the original value. The CRC method contains a check (data verification) value of redundancy (which does not add information to a message), and the algorithm based on cyclic codes. CRC method is very popular because it is easy to implement in binary hardware and it is relatively easy to analyze mathematically. This method is particularly good at detecting frequent errors caused by noise in transmission channels. Because the checksum value has a fixed length, its functions for generation of code are used occasionally in hash functions as well. CRC was invented by W. Wesley Peterson in 1961. CRC is specifically designed to provide protection associated with common types of errors in communication channels, where they can provide integrity of

transmitted data. However, they are not suitable for protection against intentional modification of data because there is no authentication required, and the attacker can change the message and rearrange the CRC without being discovered.

### **3. PUBLIC KEY INFRASTRUCTURE**

Public key infrastructure (PKI) is a set of people, procedures, programs and hardware necessary for the management, storage, modification and use of digital certificates. PKI is a security structure designed for the purpose of improving the security in the exchange of relevant information and data as well as money. PKI consists of several interconnected objects, buildings, applications, services and tools for managing and monitoring of the PKI system:

- CA (Certification Authority) that issues and verifies the digital certificates,
- RA (Registration Authority) that checks the identity of users requesting the CA
- CRL list (Certification Revocation List)
- User certificate
- Certificate management system

Public key infrastructure is implemented in order to provide:

- Accuracy and security of electronically sent or received message
- Time relevancy of sent or received message
- Privacy of transferred information
- guarantee that the information can be used in court as evidence if there is some form of discrimination of accuracy or abuse of relevant information

In cryptography, CA is an entity that issues digital certificates. In public key infrastructure, CA is an organization that stores public keys and their owners while providing protocol of secure communication to all parties by giving them a corresponding public key. For example, when a user visits an important site such as, site of a bank or relevant organizations, web browser receives a public key and the digital signature of the organization that can be used to check for the safety and integrity of the received key.

CA may use the Registration Authority (RA) to perform the necessary checks of the person or organization requesting the certificate in order to ensure their identity.

A digital signature is an electronic security mark that can be assigned to files. It allows verification of identity of parties that issue out files and information and checking whether the files and information are altered in any way from the time when they are digitally signed. If the file does not have a valid digital signature its legitimacy is not guaranteed. In this case, it is recommended that these kinds of files are not open unless it is completely certain that source they come from is harmless. Even the correct digital signature does not guarantee that the contents of the file are harmless and that the files are not altered in some way. In cryptography, digital certificate represents an electronic document using a digital signature that binds a public key with an identity - information such as the name of a person or an organization, their address,



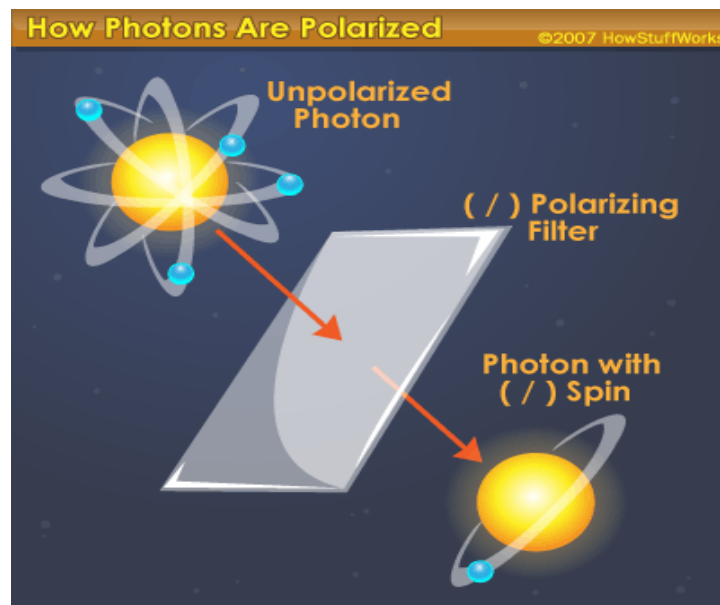
etc... The certificate can be used to verify that the public key belongs to an individual. A digital certificate contains the following elements:

- serial number – unique serial number of certificate
- subject – name of the organization of individual
- signature algorithm – algorithm used to generate a signature
- signature – the actual signature that serves as confirmation that information comes from the party that issued the signature
- issuer – entity which issues the certificates
- usability – time of validity of certificate
- purpose of key – purpose of use of key
- public key

#### **4. *QUANTUM ENCRYPTION***

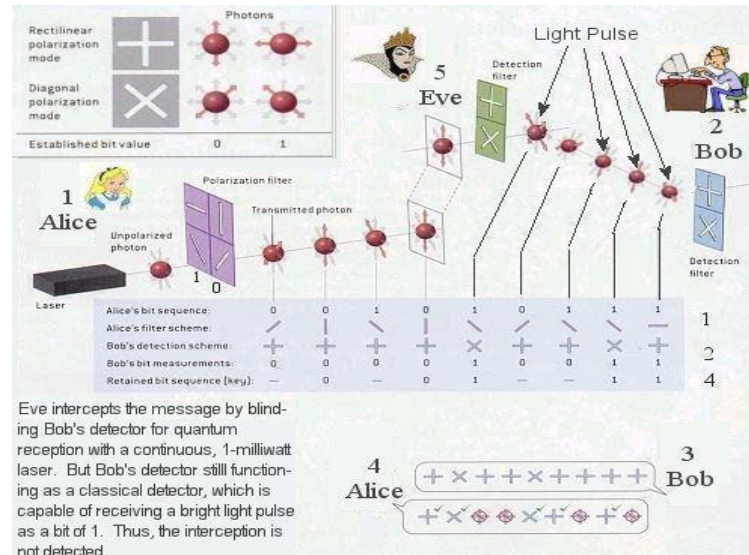
Quantum cryptography was first introduced by Stephen Wiesner at Columbia University in New York, who in the early 70s of last century, introduced the concept of quantum coding. His work, entitled "Conjugate coding" was rejected by the journal IEEE Information Theory, but still gets published in 1983 in SIGACT News. In this work he showed how to locate and send two messages that are encoded in two "related phenomena" such as linear and circular polarization of light, so that either, but not both, can be sent, received and decoded.. Ten years later, continuing his work, Charles H. Bennett of the IBM Research Center, and Gilles Brassard from the University of Montreal, proposed a method for secure communication, which was based on Wiesner's "related phenomena." At the same time Artur Ekert of the University of Oxford in 1990 has developed a different approach to quantum cryptography based on quantum correlations known as quantum entanglement. Quantum encryption or quantum key distribution uses quantum mechanics to allow secure communication. It allows the two sides to create a shared random bit string known only to them, which can be used as a key for encryption and decryption. Important and unique property of quantum encryption is the ability of two users involved in communication to detect the presence of a third party who tries to discover information about the key. This comes from the basic aspects of quantum mechanics: the process of measuring a quantum system essentially undermines the system itself. A third party who tries to eavesdrop on the key is causing irregularities that can be noticed. By using quantum superpositions or quantum entanglement, transmitting information in quantum states can be implemented in communication system that is able to recognize eavesdropping. If the level of eavesdropping is below a certain threshold value, one can create a key that will surely be safe (ie. an eavesdropper will not be able to obtain information about it), otherwise it is not possible to achieve a safe key and communication is interrupted. Safety of quantum encryption relies on the foundations of quantum mechanics as compared to traditional public key encryption, which relies on the certain mathematical functions, and can give no indication of eavesdropping or guarantee for the security of issued key. The algorithm that is most commonly associated with QKD is a "one-time pad" and its security is verifiable when used with a secret, random key. Quantum communication involves encoding information in quantum states, or qubits (as opposite to bits used in traditional communication). Usually the photons are used to achieve quantum states. Quantum cryptography uses the individual properties of these quantum states to ensure safety. There are several different approaches to quantum key distribution, which can be

divided into two main categories depending on features that are being used. Generally, the measurement of an unknown quantum state will change this situation. The quantum states of two or more separate objects can become linked so that they can be described as mixed quantum state and not as individual objects. This means that the implementation of the measurements on an object affects another object. If a pair of intertwined objects is being sent through a communication channel, any attempt to intercept any particle will cause a change in the entire structure, which will in turn lead to the discovery of a third party, ie. These two approaches can further be divided into three families of protocols: discrete variables, continuous variables and distributed phase reference coding. Protocols of other two groups are mainly oriented towards overcoming the practical limitations in the experiments. Ekert scheme uses entangled pair of photons. They can be created by Alice, Bob or any of independent sources, including Eve that eavesdrops. Photons are distributed so that Alice and Bob obtain one photon from each pair.



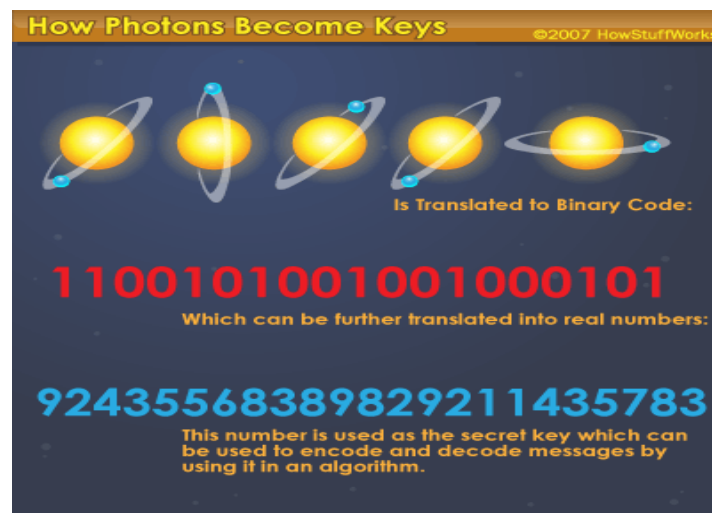
**Image 3:** Photon polarization

This scheme is based on two properties of entanglement of photons. First, intertwined states are perfectly connected in the sense that if Alice and Bob measure whether their particles have vertical or horizontal polarization, they always get the same answer with one hundred percent probability. The same is true for any other pair of complementary (orthogonal) polarizations. However, concrete results are completely random; Alice can not predict whether it will get vertical or horizontal polarization. Any attempt at eavesdropping Eve destroys the correlation between photons in a way that Alice and Bob can detect.



**Image 4:** Communication between Alice and Bob (with interference of Eve party) using quantum encryption

Previously described quantum cryptography protocols provide Alice and Bob almost identical shared keys with anticipation of divergences between the keys. These differences may be caused by eavesdropping, and imperfections regarding transfer and detectors. As it is impossible to distinguish between both these types of errors, guaranteed security requires the assumption that all errors result from interception. Considering that the percentage of error is less than a certain norm (20% from April 2007), the two steps can be implemented to remove the incorrect bits and then reduced Eva's knowledge of the key to negligible value. These two steps are known as the alignment of information and reinforcement of privacy.



**Image 5:** How photons become keys

Information polarization is way of error correction which is carried out between the keys of Alice and Bob, in an attempt to ensure the identity of both keys. The process is conducted in public channels and therefore it is important to minimize the transmitted information about the keys because they can be read by the Eve. The usual protocol is a cascade protocol proposed in 1994. It takes place in several stages, where both keys are divided into blocks in each stage and

are being compared to the parities of these blocks. If difference in parity is detected, the process of binary search is implemented to find and correct error causing inparity. If an error occurs in the block in the previous round, which had the correct parity then the error is in the same block is which is corrected as before. This process is done recursively, and after comparing all the blocks and complete all phases of Alice and Bob will have the same keys with high probability. However, Eva will also receive additional information about the key from the parity of the exchanged information.

## ***5. CONCLUSION***

Traditional methods of encryption are becoming very insecure and easily penetrable due to technical advancements of computers available today. This means that privacy of transmitted information is threatened, this becomes crucial even more if the information is confidential. The development of quantum encryption promises very great results as far as it goes to the security of the information because it is based on quantum physics rather than a pre-determined computer algorithms used in traditional methods of encryption such as encryption with the private or public key. Even though all encryption methods have certain advantages and disadvantages, it is becoming evident that, today, traditional methods of encryption are becoming less secure. In order to meet today's security requirements, quantum cryptography is being developed and promises an unexcelled level of security.

## IDENTIFYING TYPES OF ATTACK

Alen Osmanagić<sup>1</sup>, Senida Kakeš<sup>2</sup>, Benjamin Destanović<sup>3</sup>

UNIVERSITY OF "VITEZ" VITEZ

alen.osmanagic@unvi.edu.ba, senida.kakes@unvi.edu.ba, benjamin.destanovic@unvi.edu.ba

### ABSTRACT

*The current situation in the IT world is completely based on the Internet. For this reason, we must be aware of the ways and types of attacks on our network, computer, our data ... In order to protect necessary to develop awareness of how do these attacks can cause problems. Bran that, taking advices as standards for better protect.*

**Keywords:** *Computer networks, Hacker, Virus, Worms, Detection, Analysis, Operation, Spoofing*

### 1. INTRODUCTION

Computer Security is a field of computer science that deals with the supervision, monitoring and prevention of a variety of risks that could cause instability, termination of employment or any kind of damage to the software, including computer hardware.

Assuming that your computer is safe from all dangers (viruses, worms, and various types of infection), the user should be able to do exactly what they want on the computer, which is not the case if the computer is being attacked by a malicious program that is written with the intent to harm the computer run.

Backup is the way to secure data. Basically, it's just a copy of the most (or all) of the data on the computer. Data is stored on hard drives, CDs, DVDs and other media. The reserve (backup) data usually need to be kept in several places for better security, it also is possible to keep the data on a web server which probably do not know the place. In addition to threats to the security of computers, backup data is also essential if some natural disaster such as earthquake, fire and so on. The backup will be safest when you need some parasitic, like a virus, infects a file on your computer and you then your documents and the required files will be at your fingertips. With the backup of this data your documents and important files can have always, when you whenever needed.

The role of anti-virus software on your computer is to prevent the activation of known malicious applications, better known as viruses, worms and Trojan horses. These parasites hinder or even prevent the normal operation of the computer, and many of them along the way and tend to spread to other computers, which is why you have problems with your Internet provider and other customers.

Antivirus software detects malicious applications that are known to him, which makes comparing their code base so-called antivirus signatures.

Some antivirus tools offer a method called heuristics that attempt to identify the pests in their behavior, but because the author of a malicious application can test your code with antivirus software before release to the network, this method is very low efficiency. Therefore it is very important to regularly update your antivirus software definitions by visiting the manufacturer's website or by using Automatic Updates available in most antivirus tools (automatic update).

When the antivirus software detects a malicious application that wants to activate, usually ask the question what the user wants to do. Typical answers are offered to "delete", "clean", "karantenzirati" and "ignore". Usually, the entire file is malicious, which is why the option "delete" the most logical choice.

A personal firewall is an application that monitors communication between the computer and the network. Its role is to restrict the communication to that provided for normal use of the computer, thus protecting against unauthorized access. In practice, a personal firewall protects us from attempting to seize control of our computer malicious access its services. The most common form of such an approach are network worms that spread in this manner. After installation on your PC, a personal firewall monitors the activities of other applications and devices through which they access the network.

In order to simplify as much adjustment, manufacturers of personal firewall majority have decided to communicate through the network devices to share the computers we trust and with whom we share our resources (local area network) and one to which we are unreliable (the rest of the Internet). The application is similar to the case: a web browser and email client we allow to freely communicate with other computers on the Internet, while the application whose origin is not known to us usually would not allow it. Such an application may be a worm that attempts to expand or by an application installed without our knowledge that someone wants to send our passwords and other confidential information.

For unwanted applications you probably heard called spyware, adware and dialers. Protection against them is known as anti-spyware and operates on a similar basis as the antivirus software - recognize features built-definition known side applications. However, while most of the antivirus software is constantly active, protection from unwanted applications generally run on the user's request. In addition to protecting your privacy, these tools care about protecting your e-mail spam (usually e-mail addresses on the computer first thing spyware "steal").

Some of the tools for the removal, for example. SpyBot Search & Destroy, have the option of permanent protection of your web browser by removing some of its vulnerabilities and blocking unauthorized access to your home page and search settings Internet.

Because as well as antivirus software requires constant updates definitions in order to identify new forms of unwanted applications, it is necessary to new definitions frequently and regularly downloaded from the Internet via the web site of the manufacturer or installed options for automatic updates.

Security patches are usually small installation packages provided by the manufacturer of the operating system or an application is published in response to a detected failure. In this package is corrected version portion of the application in which there is an error and the code needed to replace the old solution to a new one. Users of Microsoft Windows are the most important patches for the operating system versions for the web browser Internet Explorer. Also important are security patches for tools such as a personal firewall and an antivirus program.

Security patches can be reached by visiting the page of the application you want to protect. Windows users can use Windows Update.

The codes that you use to access the Internet and electronic mail (e-mail) may not be predictable. Imagine that you have available months to try different combinations to hit someone else's code. The computer can try a very large number of different combinations of characters in a very short time. They will use dictionaries of various languages, to try all the combinations of possible birth dates, simple codes such as your user name with the possible addition of one or two letters and the like. To avoid the possibility that programs designed to hit hit your code, it may not contain predictable data. A good method of setting the password stands

6-8 characters (choose one sentence that will only make sense to you) with a throw of 2-4 punctuation marks or numbers.

In most cases, there are multiple user applications that meet specific application - multiple web browsers, multiple e-mail clients and the like. Different applications do not address the same logical problems in the same way even though the user might seem to be generally behave equally.

Because of this difference in approach, malicious code written to attack the most widespread application to another will not work. Accordingly, the use of alternative applications in their daily work significantly reduce exposure to such attacks. Alternative applications will not be without flaws, but their failures in a smaller number will be known and used in the preparation of new viruses, worms, spyware and other similar pests.

Use and regularly update security tools. Tools reduce the possibility of attack on your computer, allowing you belong in the inner circle of well-protected user. There is no perfectly protected computer, but with a little effort you will be less attractive to a potential attacker. How is Microsoft's Internet Explorer web browser is the most widespread, most malicious code is written with the intention of exploiting its vulnerabilities.

Using Mozilla Firefox or another alternative Web browser, greatly reducing the possibility of misuse of your computer. Also would on your PC should have installed antivirus, firewall, anti-spyware and alternative web browser such as Mozilla Firefox or Opera

In other types of protection includes access control. It is a way of protecting your computer where only authorized people can use a computer, usually going to the computer via password, ID cards, but lately occur much more advanced methods such as smart cards or identification by fingerprint

Encryption is a way to protect some of the messages so that someone else does not see. This can be done in several ways, for example, can scramble characters in a word or simply replace ordinary characters (letters) someone else.

Noticing the intrusion is usually technique for identifying people who are trying to enter the computer network. An example is a person who in a short time trying out several different codes on his behalf. From the first appearance of the virus in the eighties of the 20th century as well as the first appearance of unwanted electronic messages at the end of the 70s of the 20th century, the users of computer systems began to develop awareness of the need for better and better protect their computers and computer systems. How is the history of mankind has always been individuals and groups of people whose only preoccupation was causing harm to innocent people, so no computer systems were not (and will continue to be) spared malicious persons. As a result, developed a special branch of computer science that studies the security of computer systems. The objectives of this branch of computer science are wide, but there are four main objectives of research. The main objectives of the research in this branch of computer science are:

- testing of security risks in computing
- consideration of available protective measures and controls
- raising awareness of information security
- Identification of areas where more work is required to achieve better security

The main techniques for protecting computer systems are:

The main techniques for protecting computer systems are:

- User Authentication

- Access Control
- Monitoring records
- non-repudiation communication
- confidentiality of information
- integrity of information
- Availability of information and computer system

The last three items have been throughout the history of computer security proved to be three basic items in the development of secure computer systems. The need for high-security computer systems has encouraged the development of operating systems that are designed with the intention to be sure, and using all the principles derived from research on the security of computer systems. The most famous such operating system is CapROS (Capability-based Reliable Operating System) which is based on the principle of opportunity and open the original text. Any object in the model of the operating system is associated with the possibility of access rights that tells whether a facility's ability to access any other information.

## 2. *PARASITES*

Worms are usually intended to take control of your computer and allow remote control even after applying security patches. This is achieved by opening the so-called "back door" through which the author can issue commands to your computer without your knowledge. Even when the worm itself does not have malicious code, which is sometimes the case, the amount of network traffic that creates spreading can slow or even prevent the normal operation of the Internet or local network. Some worms will reach out for your passwords and personal details and put them at the disposal of the author. For example, a very common cause of slowdowns of your Internet connection can actually be worms, and do not be surprised if you get a bunch of warnings for a variety of spam messages that your computer is infected with a worm, sending millions of e-mail addresses.

Most of today's worms comes to our computers via e-mail or network services. Worms are more dangerous because they generally do not require user interaction, but independently take control of the computer and continue spreading. From them we can effectively defend the firewall, but even with the firewall is recommended to apply security patches.

This double protection guarantee satisfactory level of safety. Worms that spread through the network services you will notice as attempts to connect to your computer to the firewall blocks. In this case, they are completely harmless as an attempt to exploit a security vulnerability in your computer could not be followed. A malicious program that is called viruses recognize preferably to duplicate itself. When executed on a computer, one of the first steps of trying to find the next victim and send her own copy. Viruses of worms differ in that "infect" a file or your code added to an already existing, waiting for this file is used to re-activate it. Some viruses have replaced worms that your code entirely stored in non-volatile memory, for as secret places.

As a rule, attachments in e-mails that are not completely sure that they come from a trusted source and that they expect to deserve suspicion. If you are still with it and the executive (when viewing become active, or manage your computer), doubt becomes a necessity. Executive attachments can take the form of a multitude of sequels, but the most common are: bat, exe, pif, scr, cmd, VBS and JS.

A good way of assessing whether it is a dangerous addition to consider from whom comes this amendment, if we asked for it and we know what are the files with the extension received. If we were not continued, we should proceed with caution and make sure our message was sent from



someone you trust. Name of the Trojan horse was created by the famous story of the conquest of the city of Troy abuse of trust. Similarly, virtual Trojan horse can be represented as a game or interesting content that someone sends an e-mail message. When started, to your computer to install the application for the remote control. In addition to the e-mail messages, Trojan horses can appear in the form of files on the web or file sharing networks (P2P programs - Kazaa, WinMX, Limewire, etc.). The possibilities are endless because the method of dissemination - your trust. One of the symptoms shown by the computer on which the Trojan horse is an attempt to improve server on your computer that expected orders authors. With installed and active personal firewall, this attempt will be recorded and you will be able to stop him.

Data that you may seem irrelevant such as pages visited or content that you have filled out the survey, advertisers are saying about your spending habits. It will often be referred to these data be able to learn and access codes or other information. Applications dealing with unauthorized collecting such data is called spyware.

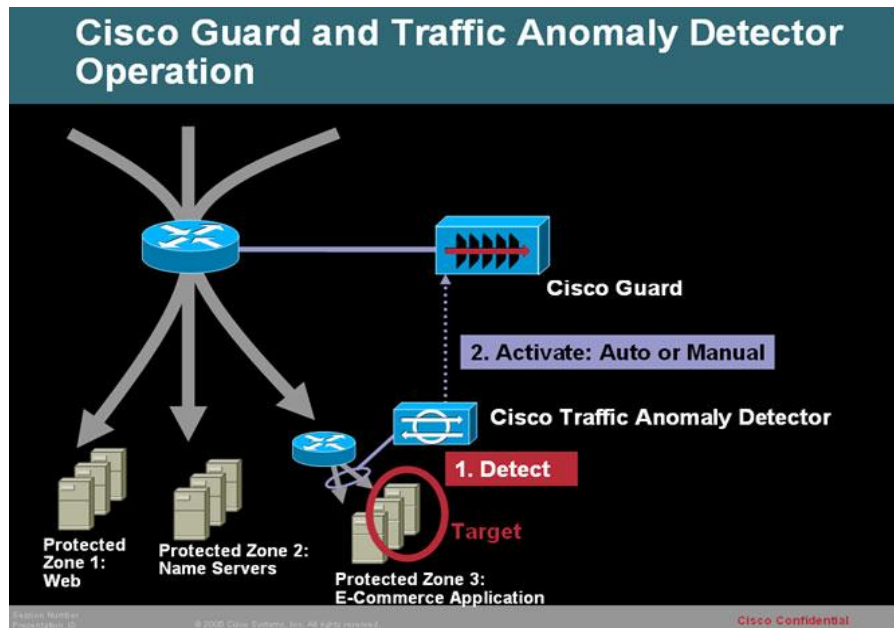
Adware is the opposite of spyware and uses the collected data to help you in as many as intrusive and show advertisements related to your habits. It usually appears in the form of countless pop-ups that appear out of nowhere while using web browser or you simply displays the page that advertises instead of the ones you have been looking for.

The largest source of spyware and adware are sites related to pornography and gambling industries, although this has not been the norm. Using omissions in your web browser and luring users to bypass security dialogues, is installed on your computer without your explicit consent, and in this case the most vulnerable web browser Internet Explorer. It is therefore recommended to use an alternative Web browser, such as Mozilla Firefox or Opera.

### **3. METHODS OF DETECTION OF ATTACK**

#### **3.1. Traffic Anomaly**

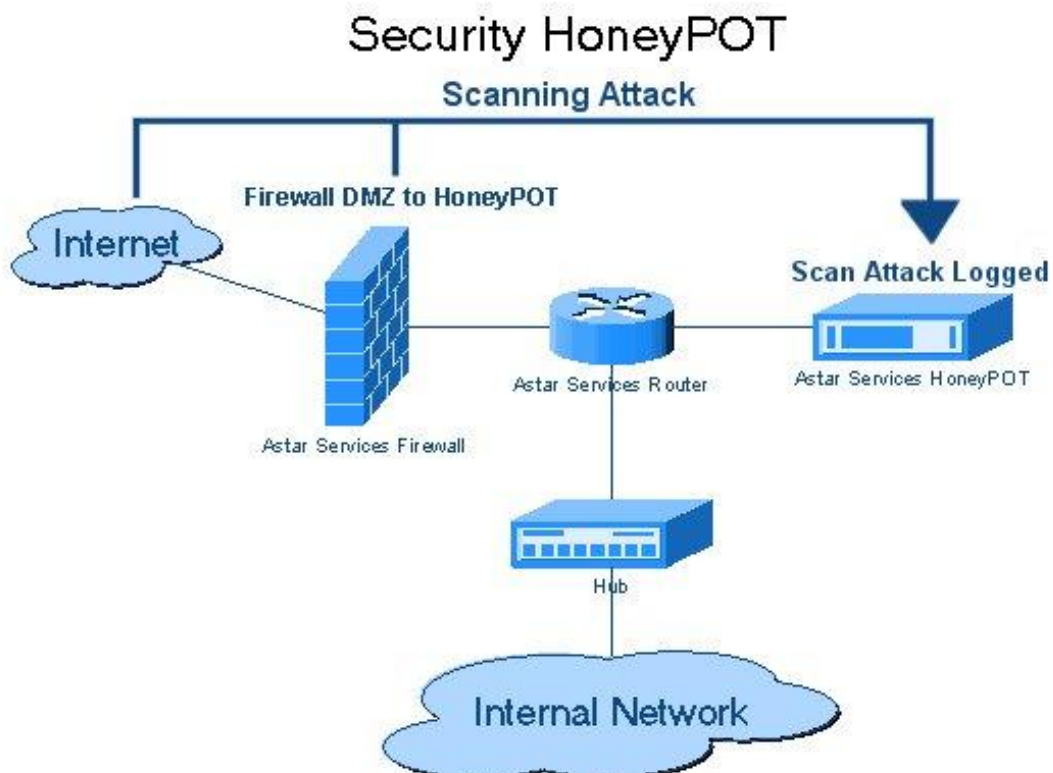
Some attacks instead of one cover several connections, mostly in the scouting phase of gathering information for future attacks. This type of detection detects unusual actions in this regard. Examples of attacks: network probes, port scans - Attack finds open ports to detect weaknesses in the system - the kind of traffic are usually indicators of attempts to collect information for the design of future attacks. If the administrator is aware of such actions on the basis of IP addresses from which you come, be prepared for possible attacks.



Slika 4.1. Traffic Anomaly Detection

### 3.2. Network Honeypot

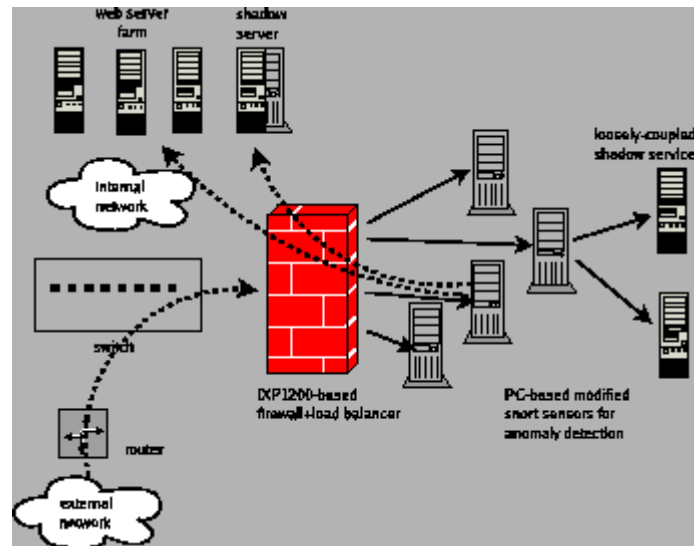
The method by which potential attackers lures to access non-existent services, which is marked as an attack due to the fact that "ordinary" network users such nonexistent services would not have approached. The system sends false information to people who scanned the network and then deny access if the record retry approach or missing resource.



Slika 4.2. Network Honeypot

### 3.3. Protocol Anomaly Detection

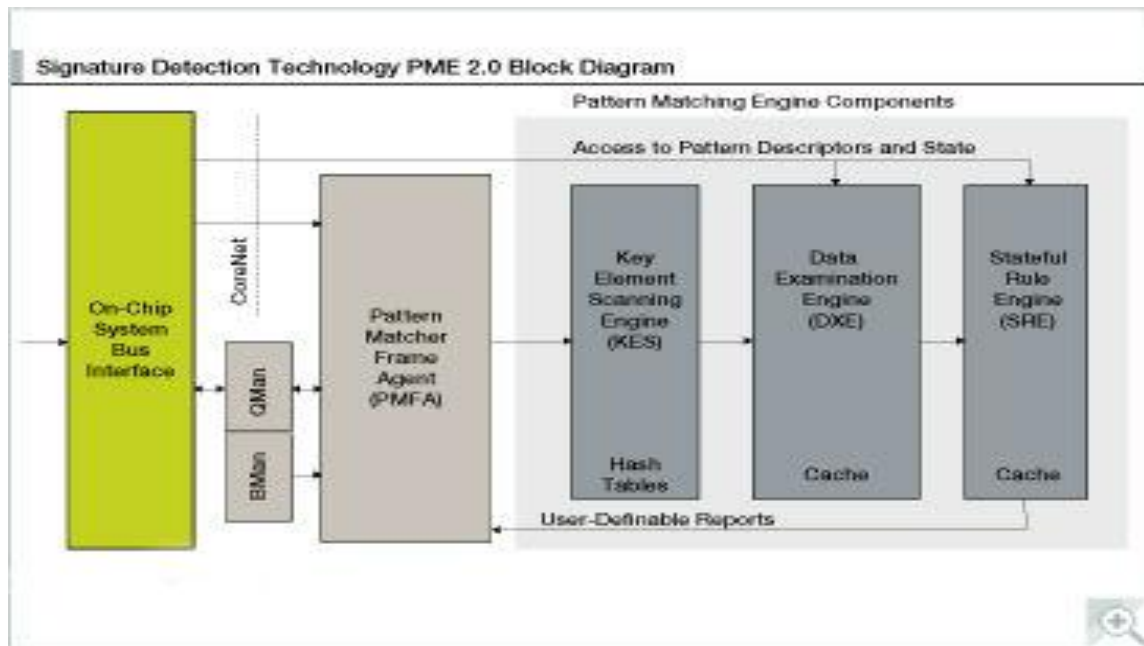
Detects attacks that deviate from the protocol used in "normal" traffic. Eg. Sendmail is a program that allows attackers to clogging mail servers to perform code for entry into the server. This type of detection compares the allowable amount of traffic to that required and prevents clogging servers and alarms on the completion of the attack. This method is effective as long as the protocol supports. Juniper IDP first in the world supporting over 60 protocols including SNMP (protection from over 60,000 threats) and SMB protection windows-based threats.



Slika 4.3. Protocol Anomaly

### 3.4. Stateful signature detection

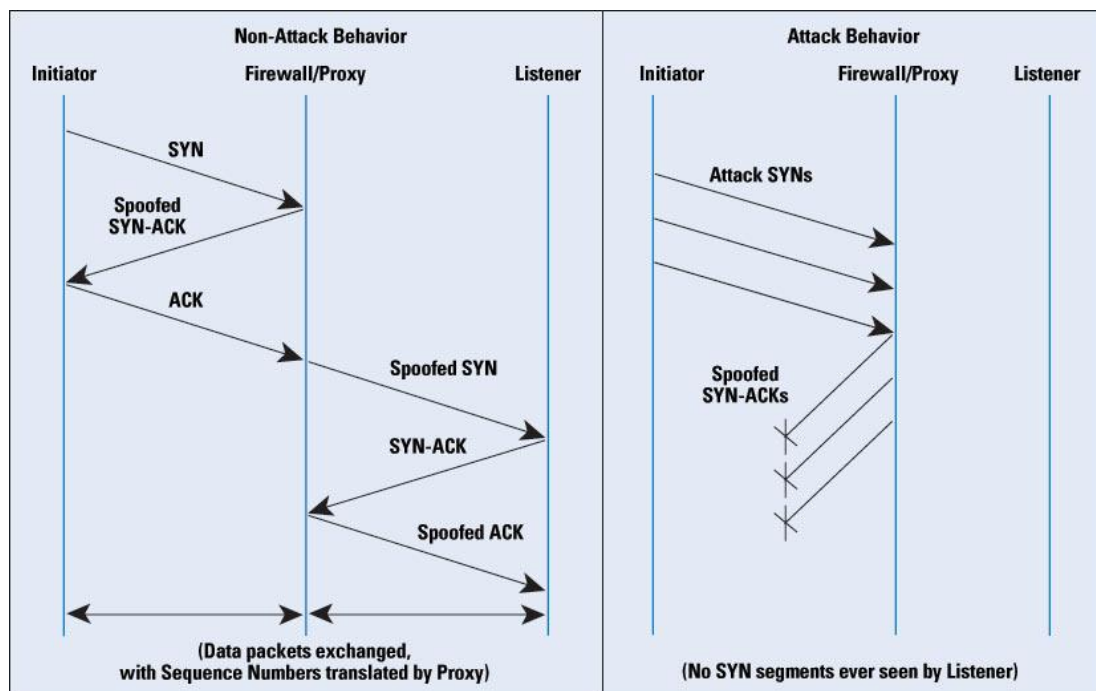
Some of the attacks can be detected from a sample found in network traffic. Classic systems based on this type of detection checked each segment in this traffic, while Juniper is observed only one in which the sample may include reducing the possibility of false alarms and increasing performance. Eg. if someone tries to log on to a specific server as the root user, the traditional IDS alert every time a traffic finds the word "root", while the Juniper IDP to do so only if the "root" is found in the login sequence which is the correct way to identify attacks.



Slika 4.4. Statefull Signature Detection

### 3.5. Syn Flood Protection

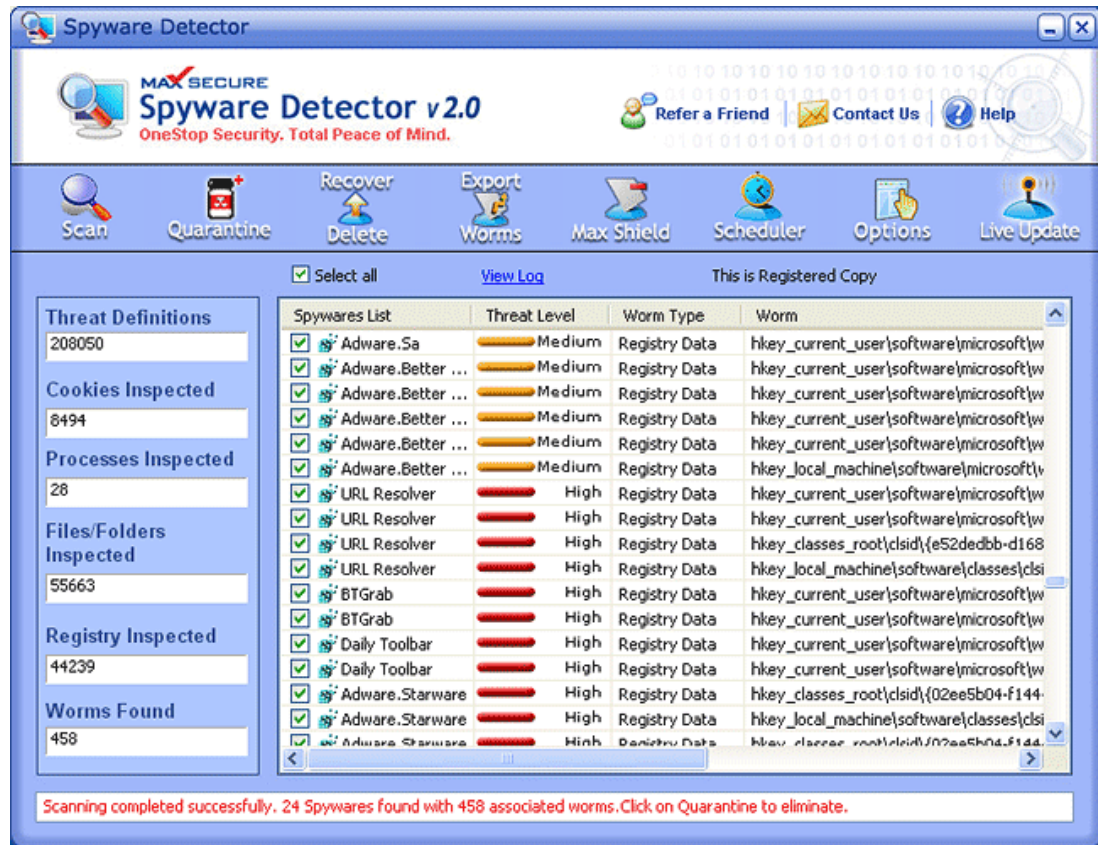
When syn flood attack server is swamped requirements for incomplete connection resulting in a DoS (denial of service). Burying a host or server connections which can not be executed, the attacker also full memory buffer. When the buffer is filled, can not be established further connections which can impair the operating system. Using Juniper IDP ahead of the sensitive parts of the network that the attack is prevented because the connection does not end as long as it has not completed the entire sequence. Therefore, syn flood attack blocked while other traffic can safely pass.



Slika 4.5. Syn Flood Protection

### 3.6. Spyware Detection

Spyware installs a companion program on your computer that sends unauthorized statistical and personal data to another person (the attacker). Spyware can be installed with the help of viruses, install a program, p2p programs, or websites. Juniper IDP detects this kind of attack through a stateful signatures methods set out in the rule base. You can identify the origin of such traffic and block it.



Slika 4.6. Spyware Detection

### 3.7. Backdoor Detection

Backdoor attacks allow an attacker to enter the network and take complete control over it, which often leads to the loss of data. Eg. Attack via email and exe files (birthday card) sends the recipient Trojans. Opening the file Trojan installs the malicious program (backdoor) without the user's knowledge. The attacker then use this program to open access to the network and assume full control over it and behind the firewall. Juniper IDP recognizes the unique characteristics of interactive traffic and sends an alarm about the unexpected actions. This type of detection can be used for:

- searching for interactive traffic
- detect unauthorized interactive traffic based on what the administrator defined as allowed
- detect almost any backdoor programs even if the traffic is encrypted, and the protocol available

```

Router#show run | begin ntp
ntp maxdistance 4
ntp server 192.168.0.1
!
end

Router#

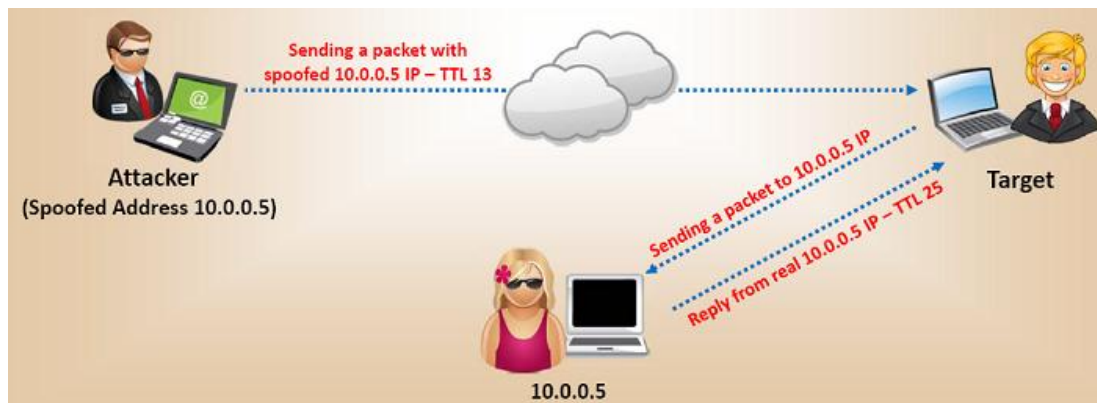
Router#

```

Slika 4.7. Backdoor detection

### 3.8. IP Spoof Detection

IP spoofing is a technique used to facilitate unauthorized access to computers in a way to interfere with the IP address so that it appears as if the message comes from the inside (from the network). This kind of detection was included in the final phase of the attack because it requires that the attacker has a network of IP addresses to help you gain access to the network. Juniper IDP can detect such packets.



Slika 4.8. IP Spoof Detection

### 3.9. Layer 2 Attack Detection

A good example of Layer 2 attack is ARP spoofing. ARP is an abbreviation of the term Address Resolution Protocol and is a standard way to IP and Ethernet work together to direct the packets to where they should go. ARP request "asks": "Is your IP address xxxx? If so, send me your MAC address. ARP spoofing involves creating fake ARP response, which allows an attacker to perform man in the middle attacks persuading computer A to computer B is on and vice versa. Target computers are considered to communicate with each other, while all traffic is actually going through the attacker's computer. Juniper IDP can detect these types of attacks.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping armanasci.com

Pinging armanasci.com [10.0.0.8] with 32 bytes of data:
Reply from 10.0.0.8: bytes=32 time<1ms TTL=64
Reply from 10.0.0.8: bytes=32 time<1ms TTL=64
Reply from 10.0.0.8: bytes=32 time<1ms TTL=64
Reply from 10.0.0.8: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\DELL>_
```

Slika 4.9. Layer 2 Attack Detection

#### **4. CONCLUSION**

Protecting the computer the average user is based in fact in daily work, updating software and using antivirus solutions to minimize risks to the user's computer is infected and to prevent unauthorized modification, deletion or data usage. But as far as the user for information systems, the best way security is actually to implement systems that are created just for the sake of a higher level of security. Of course this could be an expensive solution, but most turned out to be valid. But, again, the question regarding safety when we are online, we are vulnerable. No matter what you use, your computer can easily be infected. Because there is no system nor software solutions that we can guarantee 100% security. Another thing that can be concluded as correct that now Linux's systems (Ubuntu) are the safest. At least those that are not commercial, but it again raises the question of what any user needs. That is why we are not yet able to say that the security of the computer unquestionable

#### **5. REFERENCES**

- [1] [https://bib.irb.hr/datoteka/361852.diplomski\\_rad.pdf](https://bib.irb.hr/datoteka/361852.diplomski_rad.pdf) (10.12.2013.)
- [2] [http://nastava.unvi.edu.ba/file.php/144/Analiza\\_sigurnosti\\_IS.pdf](http://nastava.unvi.edu.ba/file.php/144/Analiza_sigurnosti_IS.pdf) (10.12.2013.)



# APPLICATION OF IT AND IT TOOLS IN MEDICINE, MYCIN

Sead Hamzić

Kladanj

sead.hamzic@unvi.edu.ba

## ABSTRACT

*In this work covered by the medical informatics. So, briefly told what actually constitutes a medical informatics, which is the purpose of the introduction of information technology in the field of medicine. We will see what are the most notable examples of the application of computers in the computer field. Particular emphasis is placed on the EC MYCIN, a tool that assists physicians in diagnosing infectious diseases of the blood.*

**The keywords:** *The expert system, MYCIN, medical informatics.*

## 1. INTRODUCTION

In short answer to the question what is medical informatics is not easy because the diversity of topics that covers does not allow easy use.

Modern approach to information science based on communication, so we can say that medical informatics in the broadest sense studied determinants and contemporary methods in medical language and medical communication.

Every day, professionals in various professions in collaboration with computer scientists are discovering ways to apply computers, increasing the effectiveness and the efficiency of any in a given area. Computers are inevitably helped many walks of life and have become an indispensable instrument for working in a number of professions. Whether we like it or not, this process is unstoppable and getting more and more momentum. Paper, film and media similar to retreat before the upcoming digital replacements. Former figure medical offices to which we are all accustomed to, with drawers full medical records, prescriptions, instructions ... becomes history. At their tables you apart from the usual instruments only see the LCD monitor which will in a split second will be able to find out everything about the patient: when you removed the first tooth, when you had the flu when you were on sick leave ... With one click of the mouse and your employer would also have to have all this information on your computer. This is the future that is coming relentlessly, even in our country which is considered to be an information on the back. In addition to the files and administrative tasks computers in medicine are increasingly and responsibilities in the diagnosis, treatment, training. As in any other area in which they are used, it is clear that yields many benefits, but also bring new types of problems that must mean de adapt and find an adequate answer. As most of them are safety issues and preserving large amounts of confidential patient data. We all went quickly in the process of digitization, now it should be to find ways to live with it.<sup>1</sup>

---

<sup>1</sup> <http://www.sk.rs/2003/03/skpr01.html>



## **2. LEVELS OF APPLICATION PROCEDURES ON MEDICAL INFORMATICS**

The use of computers in medicine is based on an intent to improve in every aspect of providing medical care to patients. The physician in this environment takes on a whole new tasks, partially or even completely relieved some of the work but still remains irreplaceable individual. In terms of intellectual work of doctors joining the IT period does not become easier but on the contrary, more complex and demanding. For clarification degree of computerization of medical science computers Bommel describes six levels of their application:

- Communication and Telematics,
- Storage and retrieval of data,
- Data processing and automatization,
- Diagnostics and decision making,
- Treatment,
- Research-and-development <sup>2</sup>

As technology advances, more and more different medical areas in your practice begins to rely on computers. However, several years ago, in the world and in our country, the use of the computer has been established in certain areas of medicine, and even became a regular practice. These areas can be broadly divided into four: diagnostics, special types of therapy and surgery, telemedicine and administration. As time passes, both are born better systems that gently begin increasingly to blur these boundaries. The "digital path" from diagnosis to treatment is becoming shorter and faster. The most notable examples of the application of computers in medicine relate to the diagnosis and telemedicine. Particularly in these other areas has come to the fore a combination of personal computers and the Internet. Modern methods of diagnosis, such as computed tomography, magnetic resonance imaging, endoscopy, digital x-ray and ultrasound are infeasible without special hardware and software. Appliances CT, popularly called "scanners" are working on the principle of X-rays, except that the radiation is focused. "Head" is a computer-guided scanner and circling around certain areas of the patient and a real thin "snit." Due to the passage through the tissue of different density, X-ray radiation becomes more or less absorbed, and the sensors in the form of a tunnel in which the patient is performed sensing signals. Computerized system based on the obtained values form a series of horizontal section of a certain part of the body and displays them on the screen. Following a similar principle work and other high-tech methods of diagnosis, or the application of computers in medicine has its own specific requirements to which we turn. Most computerized diagnostic device receives at its output some kind of image. And as you know, whenever it comes to some sort of digital images, as their quality is higher, the higher and their size. Thus, it is clear that some kind of medicine that image by making the most handled. But the image that represents a snapshot of an organ can not be bad. On the contrary, it must be as good as possible and with the best possible resolution in order to set the proper physician diagnosis. IT specialists who deal with computing in medicine have proposed a new image format that is obtained at the output of most computerized diagnostic devices. DICOM Standard. (Digital Imaging and Communications in Medicine) is created by the American Organization NEMA (National

---

<sup>2</sup> [http://mi.medri.hr/uvod\\_medinfo.htm#2stojemedinfo](http://mi.medri.hr/uvod_medinfo.htm#2stojemedinfo)

Electrical Manufacturers Association). The purpose of the new standard is to assist medical professionals in obtaining, using and sharing shots from different sources: scanners, magnetic resonance, ultrasound ... DICOM file in terms of structure consists of two parts: the first is a header that contains text information (name of the patient, the type of review, the image data, etc.), While the second part of the file containing the image itself, which can be three-dimensional. This is one of the most commonly used standards in medicine. Unfortunately, no commercial software for image processing is not supported. To see DICOM images of organs and body parts must have special software. As we noted, the standard DICOM provides high image quality and adapted to specific requirements. However, the file sizes can be significant in some situations mentioned the size of 80 MB. Before Informatics in Medicine this sets the first of the specific demands - enable systems that can store a large number of these images to them at any moment to deliver insight on any workstation in the system, as well as to provide cheap and safe storage of images in the long run . Another very important point in this chain is the monitor. Doctors no longer have the classic X-rays in their hands, which will study the opposite light source - before they will monitor. Monitors that are used in the diagnosis can not be any monitors: only if they show is not good enough, the doctor could be a mistake in the diagnosis, and it may cost someone life. Accordingly, the three characteristics necessary for such monitors are: the greater the resolution, the greater the visible surface, the possibility of large contrast values, as well as the ability to display a greater number of shades of gray. Why shades of gray? As we know, X-rays were always black and white, so are on the screen. The increasing use of new computerized method in medicine every day creates an ever larger amounts of data that must be stored somewhere for a longer period, but also provide quick and easy access when needed. Many large companies are competing with each other in this field by offering a different good (and expensive) solutions. Hardware and software in these systems until recently were the only "owner" that is closed source. However, in recent years more and more is in this area of IT is present with its Linux open source solutions. So a group of researchers from Germany, constructed a system that relies entirely on open source solutions. This system is called "Marvin digital archive," it is cheap compared to the competition, is easy to use, and how hard it is very fast in operation. Created by researchers at the Department of Radiology, Hospital Berlin "Charité. The system saves all images of different diagnostic views on a series of servers that can be accessed over a local network or through the Internet using a Web browser. The system works by Central Image Server receives radiological images in DICOM format, as well as the usual information about the patients. In a separate series of servers are kept in these pictures and the information that can later be delivered either via HTTP, either as DICOM images. When both free memory space are added new servers. But given that the hospital "Charite" creates 9.6 GB of radiological images a day (!), The need for new servers is obvious. The team hopes that the emergence of new high-capacity hard drives significantly reduce the need for new servers, because the servers improvement disks larger capacity, to be able to place an even greater amount of data. The current system capacity is 4.8 TB. Of course not everything is perfect: the cost of the formation of this system are estimated at 70,000 euros, and it is assumed that the lifespan of the hard disk for storing data three years, after which it is recommended to replace them and copy the data to another media. Where there is money, there is room for innovation. . Another example of the introduction of new technologies in medicine comes from the university hospital "Oulu" in Finland. There they tried to wirelessly networked entire complex, allowing staff to the fastest way to access all kinds of data on patients. Specifically, there are two variants: the first order in each bed was provided with an Ethernet port where the doctor joined with his laptop and called for all necessary information on the respective patient. The whole procedure should be repeated for each bed. But the idea was

rejected before it actually works, because it was obvious that the more doctors to deal with cables and IP addresses rather than patients. However, hopes are placed in wireless networking: every doctor should have a notebook or tablet PC equipped with software CHILI ([www.chili-radiology.com](http://www.chili-radiology.com)) that enables viewing of DICOM images from a variety of modern diagnostic equipment, while at the same time allows and teleradiology. The doctors at this wireless variants reacted much better, but the main zamijerka they were little autonomy used version Tablet PC, (battery life is short), and the lack of speed. Given the fact that the images they work with rather large, take some time to get those loaded via the wireless network, which is slower than a conventional networking. All in all, the process of creating a "paperless" medicine is not going smoothly in rich environments, and many experts in this field wonder whether this new solution actually bring savings that are "trumpet on all sides."<sup>3</sup>

### 3. MYCIN

One of the oldest known expert systems MYCIN was developed in 1972 at Stanford University in the USA. The EC has been developed on a PDP-11 computer and contains over 500 rules and relations, and is designed as a powerful tool physicians in diagnosing infectious diseases of the blood. For example MYCIN's may be a good analysis of the work of the EC. To make it easier to follow the dialogue between users, or the doctor, and the EC, respectively MYCIN, the following abbreviations are used:

- OSD: doctor - user,
- EIR: an expert system.

The dialogue between the user and the EC.

After turning on the computer and calling the EC, there is MYCIN and begin dialogue.  
EIR: GREETINGS MYCIN

Want to instructions (YES or NO)?

KOR: YES

EIR: MYCIN expert system is designed for consultations on issues of infectious diseases. I think you want to get information about the treatment of a patient. So I'm going to ask you some questions about the patient. If you are not quite sure of your answer, then you can in parentheses give your safety coefficient (a number from 1 to 10). The number 10 corresponds to the absolute conviction. If you want to change the answer to any of the preceding questions, give the command CHANGED, behind which must follow a number of questions to which you want to change an answer. Not apply this command often, because after her system approach to verification from the very beginning (even if not to spell new user questions), all of which increases the time for obtaining solutions. One possible response to the question of the system, you can do the following information:

First from (uncertain) - if you do not know the answer to the question that you gave the system;

---

<sup>3</sup> <http://www.sk.rs/2003/03/skpr01.html>

Second? - If you want a system that a possible answer;

3rd ?? - If you want a system that all possible answers to the question;

4th PR (RULE) - if you want a system appears to rule on the basis of which he gave an answer to the question;

5. Why - if you want a system further explain the rules by which he came up with the answer to the current question;

6. HOW-N - if you want an explanation of how the system came to the finish line after N protection issues;

7. In - And - if you want to interrupt consultations to set a system of additional questions and information

If you are in the course of consultations forgotten permitted command or action, select the command HELP (HELP) and the system will immediately help.

End of instruction.

Example of use MYCIN's

Once the user has got this and similar instructions (telling the user in any case need not be a computer specialist), can be accessed by the practical use of MYCIN's. In the following day is an example of this usage.

EIR: 1. Name of the patient?

KOR: Niko Nikić

EIR: 2nd Gender?

KOR: Male

EIR: 3rd Age (years)?

KOR: 47

EIR: 4. Are the resulting culture of microorganisms from infected places?

KOR: YNe

EIR: 5. What is this infection?

KOR: Primary, bacteria

EIR: Please sixth date of the first symptoms of infection (infection-1) - (month, day, year)

KOR: May 10, 2003

EIR: 7. For which of the resulting culture?

KOR: From the blood

EIR: 8. When was obtained for the crop (month, day, year)?

KOR: May 14, 2003

EIR: 9th microorganism identified?

KOR: No

This kind of dialogue continues until the system fails to collect enough information about the patient. Further dialogue will be skipped and will be shown its completion.

EIR: 45th therapeutic recommendations are based on the fact that the infection is actually the primary bacteriological and that the micro-organism:

1st Pseudomonas - aeruginosa

Second klebsiella - PNEUMONIAE

3rd E. coli

4th Bacteroides - fragilis

5th ENTEROBACTER

6th PROTEUS-NON-MIRABILIS

How to evaluate the state of the patient (using a scale from 0 to 4, where the large number of poor

KOR:3

EIR: 46. Has the patient Savo Savic on the performed search showed Allergy reaction to any antibiotic?

KOR: No

EIR: 47. What is the weight of the patient?

KOR: 70

EIR: 48. RECOMMENDATIONS 1. My first recommendation is as follows:

To solve cases <1, 2, 3, 5, 6>:

Prescribe: Gentamycin

Dose: 107 mg (1.7 mg / kg) every 8 hours intramuscularly or intravenously for 10 days.  
Comments: Modify dose in case of unsatisfactory effect.

In order to solve the case <4>:

Prescribe:Clindamycin

Comment: If the diarrhea or other gastrointestinal - indigestion, immediately check the patient's presence pseudomembanskog-kolita.

After this MYCIN asks the user for further, more detailed, consideration and, possibly, new facts. This small example illustrates the method of communication and a form of labor EC. During the dialogue is collected facts, take a detailed and less detailed data and come up with the required solutions.

After this immediately raises the question of how one ES reliable, or how much he can really trust. Conducted numerous investigations of the quality of the EC, the first MYCIN's and later and later others, and all the tests have given more than outstanding results.<sup>4</sup>

### **3. CONCLUSION**

The future of medical informatics seems very promising. Number of health facilities daily showing more interest in the introduction of information technology in health care. Computer technology is much improved from the time when the support systems were initially therefore can certainly be helpful when it comes to their example in health care. All this, and the need for efficient management and storage of medical data, indicates that such applications will be developed and used in Future.

### **4. REFERENCES**

- [1] <http://www.etf.ucg.ac.me/materijal/1190371410ES.pdf> (02.11.2014)
- [2] <http://www.infoteh.rs.ba/rad/2012/STS/STS-21.pdf> (03.11.2014)
- [3] [http://mi.medri.hr/uvod\\_medinfo.htm#2stojemedinfo](http://mi.medri.hr/uvod_medinfo.htm#2stojemedinfo) (03.11.2014)
- [4] <http://www.sk.rs/2003/03/skpr01.html> (03.11.2014)

---

<sup>4</sup> <http://www.etf.ucg.ac.me/materijal/1190371410ES.pdf>

