Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, December 2012, vol. 17, no.3
(http://www.arraydev.com/commerce/jibc/)

Safety of e-business Applications in Serbia: Applied Knowledge Based on SSL Traffic

MARKO SARAC
Teaching assistant, Singidunum University, Belgrade, Serbia
Postal Address: **Singidunum University, Danijelova 32, 11000 Belgrade, Serbia**
Author's Personal/Organizational Website: www.signidunum.ac.rs
Email: **msarac@singidunum.ac.rs**

Marko Sarac is a PhD Research Candidate and Teaching Assistant at Faculty of Informatics and Computing, Singidunum University, Serbia. His current research interests are Computer network, Computer networks security and Operating systems.

TIJANA RADOJEVIC
Assistant professor, Singidunum University, Belgrade, Serbia
Postal Address: **Singidunum University, Danijelova 32, 11000 Belgrade, Serbia**
Author's Personal/Organizational Website: www.signidunum.ac.rs
Email: **tradojevic@singidunum.ac.rs**

Dr. Tijana Radojevic is assistant professor in finance at Faculty of Tourism and Hospitality Management, Singidunum University, Serbia. Her areas of interests are Finance, Banking and E-business.

NEMANJA STANISIC
Assistant professor, Singidunum University, Belgrade, Serbia
Postal Address: **Singidunum University, Danijelova 32, 11000 Belgrade, Serbia**
Author's Personal/Organizational Website: www.signidunum.ac.rs
Email: **nstanisic@singidunum.ac.rs**

Dr. Nemanja Stanisic is assistant professor in finance at Faculty of Business in Belgrade, Singidunum University, Serbia. His areas of interests are Finance, Corporate finance and Valuation.

SASA ADAMOVIC
Teaching assistant, Singidunum University, Belgrade, Serbia
Postal Address: **Singidunum University, Danijelova 32, 11000 Belgrade, Serbia**
Author's Personal/Organizational Website: www.signidunum.ac.rs
Email: **sadamovic@singidunum.ac.rs**
Sasa Adamovic is a PhD Research Candidate and Teaching Assistant at Faculty of Informatics and Computing, Singidunum University, Serbia. His current research interests are Computer Security, Cryptology and Crypto-Biometrics.

DALIBOR RADOVANOVIC
Teaching assistant, Singidunum University, Belgrade, Serbia
Postal Address: **Singidunum University, Danijelova 32, 11000 Belgrade, Serbia**
Author's Personal/Organizational Website: www.signidunum.ac.rs
Email: **dradovanovic@singidunum.ac.rs**
Dalibor Radovanovic is a PhD Research Candidate and Teaching Assistant at Faculty of Informatics and Computing, Singidunum University, Serbia. His current research interests are IT Governance, IT Security and Information Systems.

Abstract

In this paper the current problems of e-business in the implementation of SSL computer network protocol are presented and analyzed. Today e-business is one of the most common methods of global economy. The paper presents research results on attacks on e-business and computer systems. Authors have analyzed contemporary methods of protection and pointed out to their shortcomings. First part of the paper is in connection with the actual problems of protection of computer networks and presents the current solutions. Second part focuses on the existing problem represented in currently used methods of modern e-business systems. The problem analyzing follows two methods of attacks. Based on the research conducted during paper writing, the authors have organized two seminars on raising awareness about the problems of modern e-business and computer network systems. Based on the discussions and surveys performed throughout the seminars, new information was acquired and those data were further analyzed and presented within the paper. The aim of this paper is to present actuality of the mentioned problem and to contribute to aforementioned security deficiency resolving.

Keywords: **e-business; computer networks; SSL; HTTP; HTTPS**

INTRODUCTION

Development of e-business is related to constantly extended implementation of computer and telecommunication technologies within data processing and information transfer and sharing. These technologies have contributed to huge changes in terms of bank system functioning. Initiated processes lead to establishment of new proceedings and technologies which additionally bring along new challenges and possibilities. Furthermore, technical-financial innovations lead the way to competition intensifying in all segments. Not only reengineering of business processes in the banks occurs, but also reengineering in business processes and mutual relations amongst the banks, banks and their clients and clients and third parties.

Main goal of e-business is to connect the clients and information flow in the fastest and the most efficient manner, regardless to geographical distance thereof. The secret of modern information system lies at flexible infrastructure based on PCs, contemporary computer networks and foremost Internet. Development of information and telecommunication technologies has created conditions for globalization of business running of the banks, i.e. it led to the establishment of new distribution channels of bank services or e-business.

However, new revolution within the area of technological changes is based on the different idea from the new infrastructure forming for the automatization of banking transactions but directed towards use of existing infrastructure of public networks, Internet above all. Internet is classified within public or open networks, with free limitless access for everyone. Use of Internet for the automatization of retail-payment transactions is favorable due to low costs per transaction. However, safety of the transactions executed via Internet presents a huge issue.

Level of data protection upon exchange of e-messages presents utterly important element on the basis of which the users opt for or against use of e-transactions. Aforementioned attribute is the most typically looked at in the cases when loss, change, unauthorized insight or some other threat to the e-documents can cause significant legal and financial consequences for on-line transaction user. That is to say that various partners are involved in e-business and exchange of e-documents, therefore all of them have to have suitable level of protection (Adamovic, 2010).

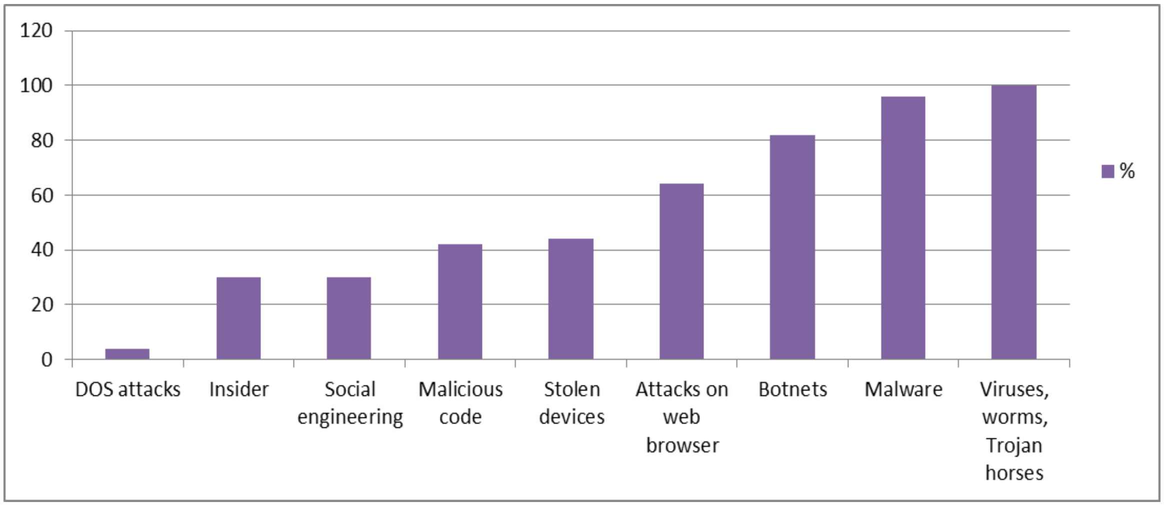
This paper investigates several mutually interconnected problems:

- Actual attacks to electronic and personal property/belongings;
- Examination of protection offered by SSL; implementation and attacks within e-business networks;
- Shortcomings of HTTPS connection establishment within e-business;
- Attacks to HTTPS traffic within e-business;
- Analysis of the discussions and surveys from held lecturing and consultations.

In the previous period we have held two lecturing's on the issues within protection of wireless computer networks in e-business. Lecturing's and survey were supported by the Ministry of Science and Technological Development of Republic of Serbia through the project TR32054 – Digital processing within the system synthesis for information protection. Lecturing's were organized on the basis of one-day seminars with the different target groups. First seminar was organized for the group of high-schools and students, while the other was organized for the group of post-graduate students as well as for the employees within both public and private sectors. Aim of both seminars was education, problem indicating but also sampling of the group which participated in the mentioned seminar. Results were collected with the method of survey conduction upon the lecturings and the same were presented and analyzed in the paper part related to the analysis of surveys of seminar participants.

DATA ON ATTACKS TO ELECTRONIC AND PERSONAL PROPERTY BELONGINGS

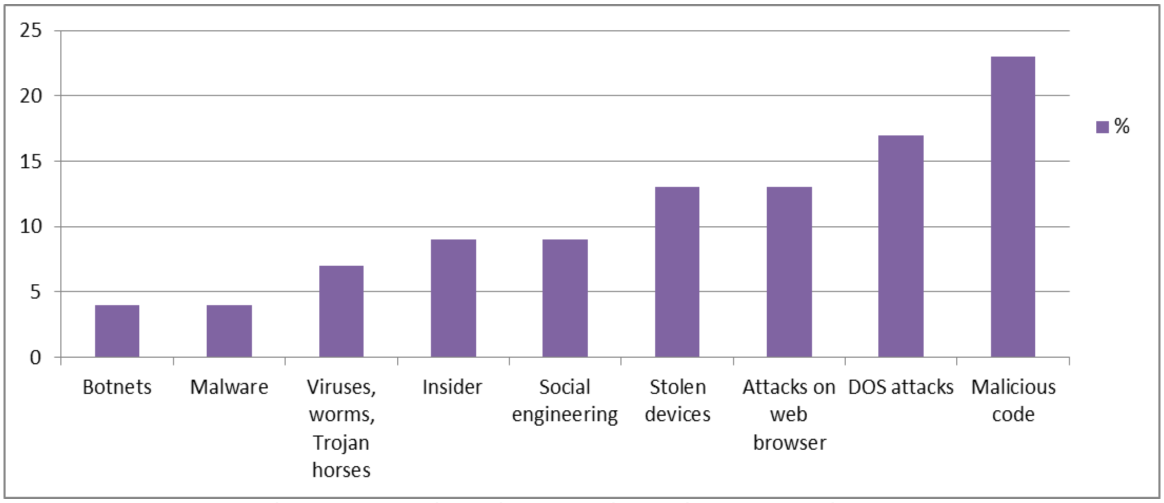
It is well-known that increasingly more and more jobs and areas within our lives depend on PCs and task carrying out via computer networks. Therefore, increasing number of researchers constantly conduct analysis and surveys related to the safety of computer systems and business transactions. Cases to follow are to show global statistical data of the most frequent attacks to computer systems, frequency of different attacks, financial damage which the bank may suffer, as well as how many days the bank needs to realize that it has been attacked.



Picture No 1: Frequency of attack to electronic and personal property/belongings

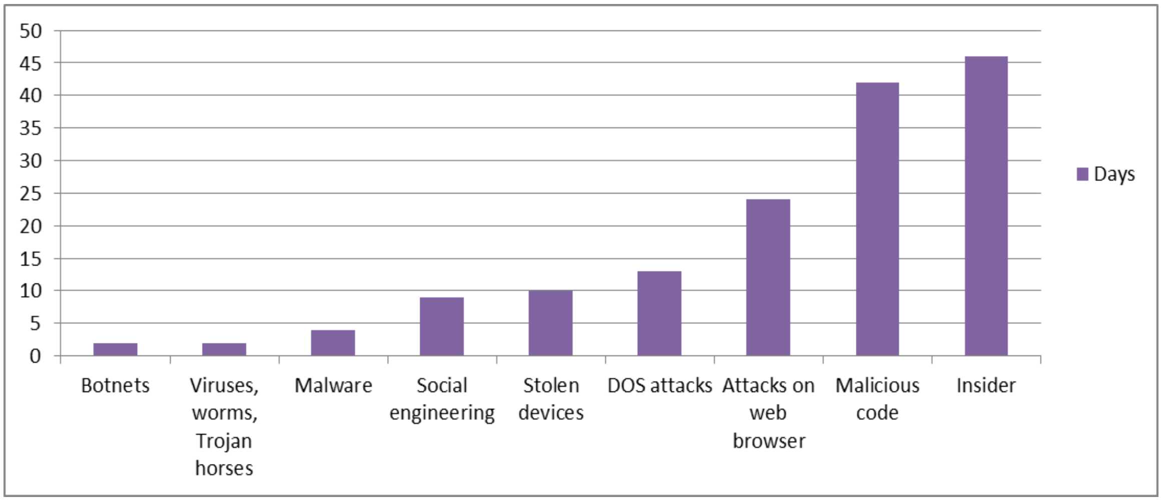
Classification per attack frequency has been displayed in picture No 1. The classification has been shown in accordance to the survey published by Ponemon Institute in August 2011 (Ponemon Institute, 2011). As the illustration presents, most of the attacks are usually conducted by viruses, worms, Trojans, malwares, while malicious codes and insiders are rarely seen as attack types. However, those rare attack kinds make the biggest financial damages to the banks.

In accordance to the data from picture No 2, and as per survey of Ponemon Institute malicious code has been identified as the biggest provoker of financial costs within the bank, while viruses, worms and Trojans which have been identified as the most frequent types of attacks retrieved only 8% out of total financial bank costs in the area of protection and attacks.



Picture No 2: Financial costs dependent on attack type

The bank frequently believes that it can function successfully and work properly even with the insider being within. This type of attack is difficult to be discovered and it takes most of the time, and relevant data in connection to the said are presented in picture No 3. Identification of the insider takes on average more than 45 days. Malicious code is also one of the biggest hardly-identified problems and it frequently takes more than 40 days until the banks realises the problem it has. This type of attack is the biggest causative agent of financial losses of the bank.



Picture No 3: Average time for attack detection

EXAMINATION OF PROTECTION OFFERED BY SSL; IMPLEMENTATION AND ATTACKS WITHIN WIRELESS COMPUTER NETWORKS

With rapid development of network applications, problem of safe transfer becomes utterly important. Therefore, use of SSL protocol becomes much more widely utilized within different network services. This protocol is not perfect by itself and problems with it frequently appear in the praxis. This part of the paper indicates the existing problem in the process of SSL connection establishment. First shortcoming with the connection establishment is use of open communication in the initial phase, hence a possibly of unauthorized content tracking exists. The other shortcoming is implementation of SSL into the application. Due to analyzing of the factor on network connection functioning, connection switch based on HTTP protocol which transfers the traffic to HTTPS is usually used. As a solution to these shortcomings, this part of the paper embraces two manners of certificate falsifications and data converting to the opposite direction in comparison to the previously desired, i.e. conversion to HTTP from HTTPS, upon which the attack is being carried out. Experiments in this part of the paper will prove that significant safety risks for HTTPS communications can be caused by more than three methods (Thomas, 2004).

Development of e-trading and cloud computing have significant impact to the implementation of SSL. Its implementation guarantees safety of communication process, and end-to-end authentication mechanisms, message encryption, checking of message integrity and other security mechanisms are in use. The biggest world manufacturers use SSL in order to protect their clients. For instance, Google protects safety of mail exchange as well as its users' applications via SSL protocol; Amazon also protects its transactions and accounts via the same SSL protocol. In the last couple of years cloud computing has recorded significant up growth in terms of use. In the vast majority of cases data exchange is conducted via SSL protocol. VeriSign, as the biggest authorization body for SSL certificate issuing, guarantees safe service use even to all the users of new Microsoft Windows Azure cloud computing platform. When cloud computing, all the data of the users as well as data processing are at a remote location, therefore connection has to function perfectly but also to remain safe in order to avoid data compromising. As it was already mentioned several times, banking sector in particular is sensitive to the attacks. This is the most interesting sector to the attackers but also the sector which service users are the most sensitive about and place where they expect the greatest security. Modern e-business mostly relies on SSL protocol as a suitable model of protection.

However, it was proven that SSL is not perfect for every type of use. Even since 2003 the first attacks to SSL protocol have been realized and mistakes in connection establishment which enabled attacks to session takeovers were proved. In 2009 Michael Howard successfully realized the attack via use of tool called Webmitm (Howard, 2009) – tool for Linux surrounding which successfully deciphers the data from SSL protocol. In the same year, the solution directing traffic from HTTPS to HTTP traffic which is easier for processing and wiretapping has been presented on the international safety conference. With these attacks a client cannot notice a difference in terms of use of services or used utilities. With further improvements, solution of attack to SSL protocol from 2009 has become one of the most frequently used ones and it will be described in greater details in this paper part.

Manufacturers of Internet explorers have been upgrading protection of their clients, basing it on warnings related to invalid sites and fake certificates. Companies for antivirus solutions have developed protections against ARP spoofing attacks, which are being the most frequently used when attacking. However, regardless of all protections and programme manufacturer initiatives, security omissions have frequently occurred and these are being used nowadays.

This paper is based on analyzing of security omissions which occur when establishing SSL connection. The analysis has been conducted with the application of two methods. First method is based on the characteristics of open text within the phase of connection establishment which was seen as shortcoming of client certification authentication, session takeover via ARP spoofing and DNS flood attack within network segment. The attacker Trojan horses server certificate forgery and presents himself as proxy or gateway, upon which the possibility for the attack occurs. The consequence of the same is that the attacker can decipher all the data transferred via HTTPS. The other method is based on the use of SSL defects and spanning of the same in the practical use. At the beginning, the attacker uses ARP spoofing to present himself as fake proxy or gateway. The attacker establishes HTTPS connection with the genuine server and that communication is further conducted with a real certificate, while the connection with deceived client is conducted via HTTP traffic which is easily tracked and processed. The attacker sends directly an open text to the client via HTTP page by deciphering encrypted data, hence he can have an easy access to all communication data.

Based on previously described scenarios several attacks have been processed in the experimental analysis with regard to their specifics. We have analyzed probability of attack successfulness and ability of the client to notice that the attack had occurred. Upon the experiment being carried out, we have executed 2 training courses, upon which we have analyzed trained clients for detection of attacks and we presented group outcome before and after mentioned training.

RESEARCH HYPOTHESES

H1: Lack of assurance about security is the greatest barrier currently affecting the growth of e-business applications.

E-business applications users must have confidence that their electronic transactions will remain private and unaltered. Consumers must trust the system to prevent fraud and keep their transactions private.

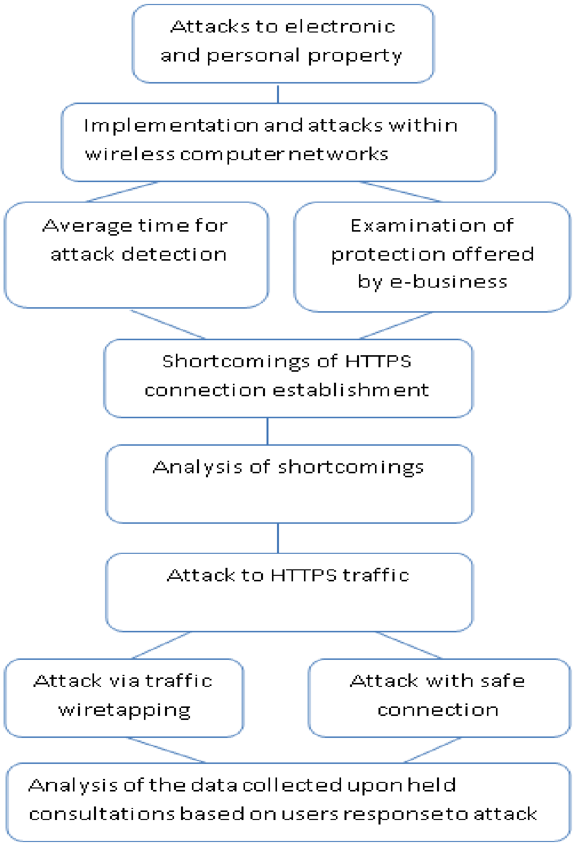
H2: E-business application security measures involve interaction of users, hardware, and software.
Because of the nature of e-business applications, we need to address all of these security issues. For example, even the best hardware network security setup might depend of user awareness of potential security breach.

H3: The model used in this research on safety of e-business applications will be able to identify security breach and alert the users on potential fraud.

RESEARCH METHODOLOGY

In Picture No 4, represented is a methodology model that was used in this work. The specified model is referring to this paper hypothesis 3. Because of poor information, the citizens of Serbia are subject to multiple levels of fraud in e-business applications. The goal of this methodology is to act preventively when there is the possibility of fraud and to identify potential problem, and to point out the elements of intrusion.

The basic assumption is that the attack is possible in all wireless networks in order to obtain someone else's property without authorized electronic access, avoiding access control systems. Based on the information gathered, users expect a guaranteed safety by theirs e-business applications. Guaranteed security is reflected in timely action to detect and prevent attacks on their own property, and that the user has the specified access levels. The methodology assumption presented in this paper in hypothesis 2 and hypothesis 3 suggests the need for a greater general knowledge to protect the safe operation of e-business applications. As part of this research a separation of two common types of attacks on the e-business applications is presented and concrete solutions are offered to detect and prevent them.


Attacks to electronic and personal property
Implementation and attacks within wireless computer networks
Average time for attack detection
Examination of protection offered by e-business
Shortcomings of HTTPS connection establishment
Analysis of shortcomings
Attack to HTTPS traffic
Attack via traffic wiretapping
Attack with safe connection
Analysis of the data collected upon held consultations based on users responseto attack

Picture No 4: Methodology model

This methodology is based on acquiring data using public conferences. Public conferences that were held, had strong consulting role, and they encouraged public discussions based on different experiences from private practice. Data was collected by the specially formulated questionnaire. A detailed statistical analysis using the method of clustering was performed. A sophisticated development environment of SPSS was used.

Shortcomings of HTTPS connection establishment

Secure Sockets Layer (SSL) is a protocol for secure message sending (communicating) via Internet. It enables sending of confidential data (e.g. credit card No) in coded and secure form via Internet. First version of SSL protocol is SSL 3.0, used for wide diapason of applications. It is comprised within IETF Internet standards. Current version of SSL protocol which is in wide use is TLS (SSL 3.1). Process of SSL connection establishment is clearly defined within RFC2246, as presented in picture No 4. A message which should be sent is received to SSL by application layer; the message is further disassembled to smaller parts convenient for encrypting, controlled No is being added, encrypting conducted as well as the compression, and then the parts are being sent. Recipient receives parts, decompression is being applied, then deciphering, checking of control numbers and composition of message parts and these are finally being submitted to the application layer.

In this manner protected channel is being achieved via SSL through the unsafe network. In case the client or server are inactive for longer period of time or the discussion with the same attributes takes too long, the attributes are being changed (Egwali, 2009).

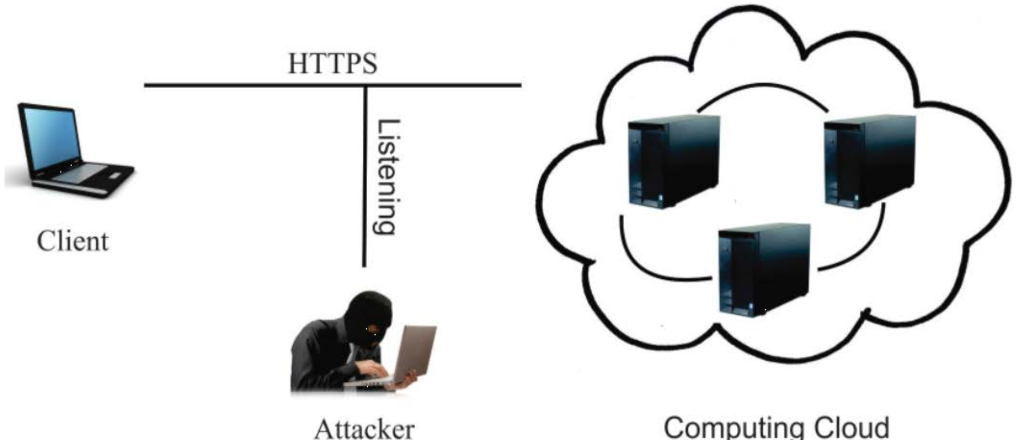
ANALYSIS OF SHORTCOMINGS

Data content is open during SSL connection establishment, thus the attacker can obtain data parcel with an unauthorized access or tracking. The attack of session takeover can occur with SSL. Client confirms server authenticity in the third step transferred by server certificate; however, the certificate is being transferred into an open text and it can be easily intercepted and used without authorization. When the attacker intercepts the message and obtains server certificate, he can copy the same and make his own fake certificate and then fill in the information with the server data. Upon that he sets his own public key and signature in the certificate and he sends falsified certificate. When the users accept fake certificate, the attack becomes successfully realized. The attacker can finally decipher premaster key which the client sends and there are no more secrets for the attacker. Therefore, there is a shortcoming in the step No 3 within SSL connection establishment (picture No 4).

As another shortcoming we can use the trust of the users in SSL and system safety. Upon various analyses, we came to the conclusion that more than 95% of the users do not pay attention when typing web-address and they do not enter HTTPS request individually. Even in the cases when the users are using HTTPS protected site access, they do not enter the address with HTTP or HTTPS part in their explorer, but simply the address as in the following form: www.sajt.com. All the Internet explorers will firstly try to make HTTP connection as desired connection type. Only upon connection with the server being established, safe-connection-adjusted servers will send a manual with redirection to the safe site like https://www.sajt.com. Furthermore, it is a frequent case that the site itself functions on the basic HTTP level without protection at certain parts (when it comes to presentation materials which do not require user interaction), and only upon user interaction need it requires safe connection for authentication purpose. These cases are mostly resolved with the setup of safe buttons which initiate safe connection. Most of the traffics function via plain HTTP traffic, mostly due to the fact that HTTPS traffic additionally burdens the servers with information encrypting. Depending on the cases, deceleration which the user notices may vary from 2 to 100 times. Therefore, systems are automatized hence HTTPS traffic is used solely for relevant data. Due to such and similar automatized solutions which facilitate everyday Internet use and use of its services, less users pay attention if plain HTTP connection or safe HTTPS connection has been established. From the perspective of the user everything seems the same, regardless of the fact if the connection was established with the entry of entire address or only the part of it; however, things function differently in terms of network traffic.

Attack via traffic wiretapping

As the initial data transfer is being conducted over open text within SSL connection establishment, the attacker can submit the data for ARP spoofing between a client and server. The attacker intercepts HTTPS request from the client and he becomes connected to the server. Upon server sending of authentication certificate, the attacker can make a certificate which would be personally signed and then sent to the client. Users tend to accept fake certificate even though programme parcels warn them not to do so due to potential deception. This makes an additional mitigating circumstance for the attack, hence the attacker can easily establish communication SSL link. The attack comprises the following steps: falsifying of ARP traffic enables interposing of the attacker to server-client relation. In that situation the attacker can monitor the traffic, i.e. parcels between the client and server. Upon ARP attack, DNS attack follows as well as wiretapping of port 443 via which SSL traffic is being established. When the attacker notices SSL request by the client, he accepts TCP request and initiates SSL connection with the server. Upon successful connection with the server the attacker prepares fake certificate which he additionally signs and Trojan horses to the client in order to further decipher entire wiretapped traffic. When the client receives fake certificate, Internet explorer might warn him on the possibility of having fake certificate or possibility of being attacked. As it was previously said in the paper, surveys have shown that nevertheless to the warning the clients most frequently accept fake certificates, if these are to lead them to desired site address. Upon acceptance of fake certificate, the attack is being considered successful since both the client and the attacker encrypt the content with the same certificate and they have SSL connection established hence the traffic can be easily wiretapped onwards. The traffic can be tracked and reviewed in the real-time.



Picture No 5: Illustration of wiretapping of HTTPS traffic

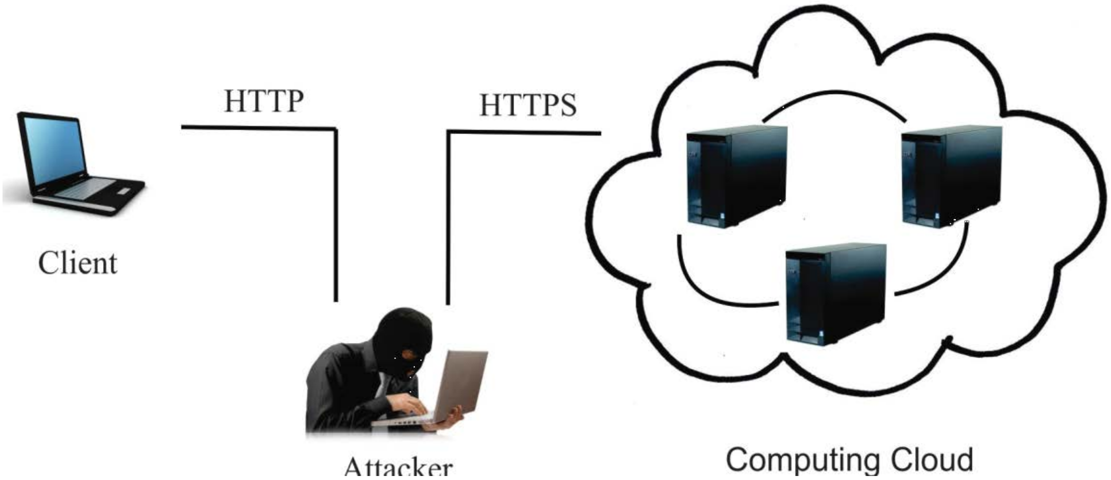
There are lots of specialized programmers for this type of the attack at present day, with the solutions including both ARP and DNS attacks. These imply graphic designs which do not require incredible know-how about computer networks and protocols. This fact enables that even undertrained individuals can become the attackers, but it also creates potentially higher No of victims. Most of Internet explorer manufacturers fight against this type of attacks with more visible warnings which do require greater interaction from the client than simple one-click-interaction.

Attack with safe connection bypassing

Similar to the first attack, the attacker can send the parcels and monitor HTTP traffic via ARP varying in between the client and server. When the attacker notices that the traffic is to be directed from plain HTTP to HTTPS traffic, he sends fake traffic to the client. On the other hand, fake HTTPS connection with the server is being established. Connection is established with truly desired location and the client receives content of desired page as the attacker received it, but the page is being sent in HTTP form without any certificates and enciphering hence the content can be still easily monitored. As the data exchanged with the client are in HTTP form and without certificate checking, there is no way that the Internet explorers can notice any kind of irregularity and warn the client, hence in this type of the attack none of client interaction is expected. Therefore, rate of successfulness of this attack is much more certain.

As it was aforementioned, detection of this attack is significantly more difficult in comparison to the previously described attack. Nevertheless, this attack type requires greater recognition of safety omissions and it is much more difficult to be implemented. The attack is graphically presented in picture 5 and it takes the following steps:

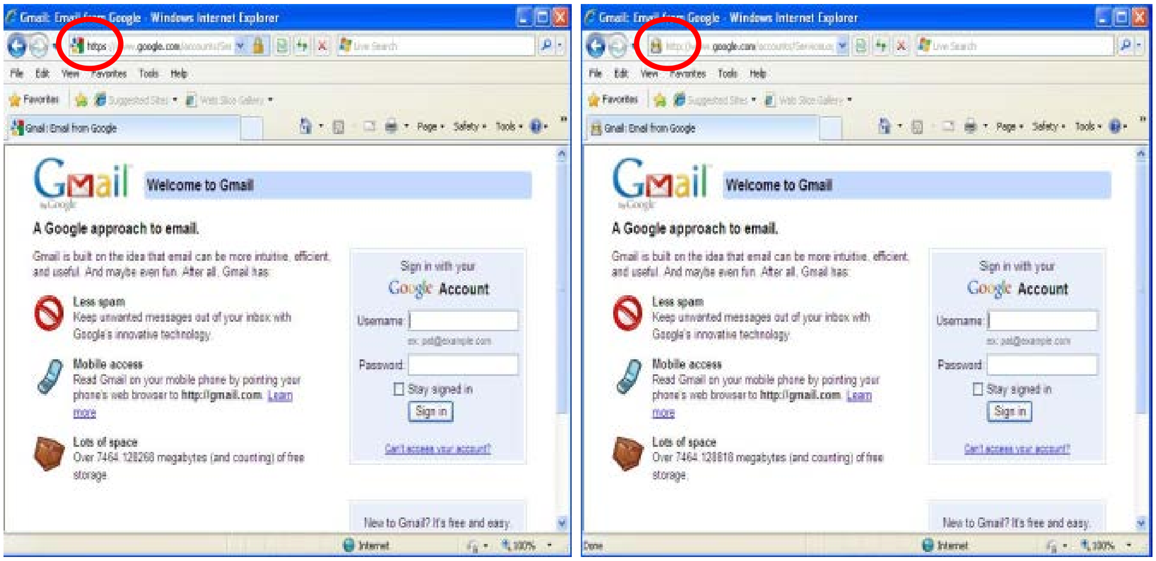
- With the conduction of ARP spoofing the attacker interposes himself between the server and client by sending fake ARP parcels to deceive both the client and server. Upon that being conducted, the attacker can send fake or valid data to both the client and server by falsely representing himself.
- The attacker tracks HTTP traffic between the server and client, thus wiretapping and analyzing the traffic.
- The attacker becomes active only upon noticing of the request for HTTPS traffic <a href=”https://...”>, upon which he changes the request with <a href=”http://...”>. If the request is presented in the following form: “location:https://…”, it will be replaced with: “location:http://…”. List of all replaced addresses is being made as well due to easier analyzing and manipulation.
- If at the later stage the attacker receives HTTP request from the client based on the inscription, he knows that HTTPS communication should be established with the server.
- Upon establishment of HTTP request with the client, the traffic becomes open (unprotected) and the only attack manifestation which the client may notice (if careful enough) is the inscription of URL address in the Internet explorer. Safe traffic in regular use would contain https in its URL address, while in the case of attack the same would contain only http in the mentioned URL address.



Picture No 6: Illustration of redirecting HTTP and HTTPS traffics

Programs being used in the second method for both APR and DNS attacks are the same as in the first method, while sslstrip and Open SSL library have been used for the removal of HTTPS traffic for the client.

Following illustration presents access to Gmail service from the Internet explorer. Unattacked connection may be seen on the left hand while on the right hand we presented attacked connection being wiretapped.


Gmail: Email from Google - Windows Internet Explorer
https://www.google.com/accounts/Se
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
Gmail: Email from Google
Page Safety Tools
Internet
100%

Welcome to Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com. Learn more

Lots of space
Over 7464.128268 megabytes (and counting) of free storage.

Sign in with your Google Account

Username:
ex: pat@example.com

Password:

□ Stay signed in

Sign in

Can't access your account?

New to Gmail? It's free and easy.

Gmail: Email from Google - Windows Internet Explorer
http://www.google.com/accounts/ServiceLo
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
Gmail: Email from Google
Page Safety Tools
Done
Internet
100%

Welcome to Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com. Learn more

Lots of space
Over 7464.128818 megabytes (and counting) of free storage.

Sign in with your Google Account

Username:
ex: pat@example.com

Password:

□ Stay signed in

Sign in

Can't access your account?

New to Gmail? It's free and easy.

Picture No 7: Internet explorer screen appearance, with and without the attack to the client

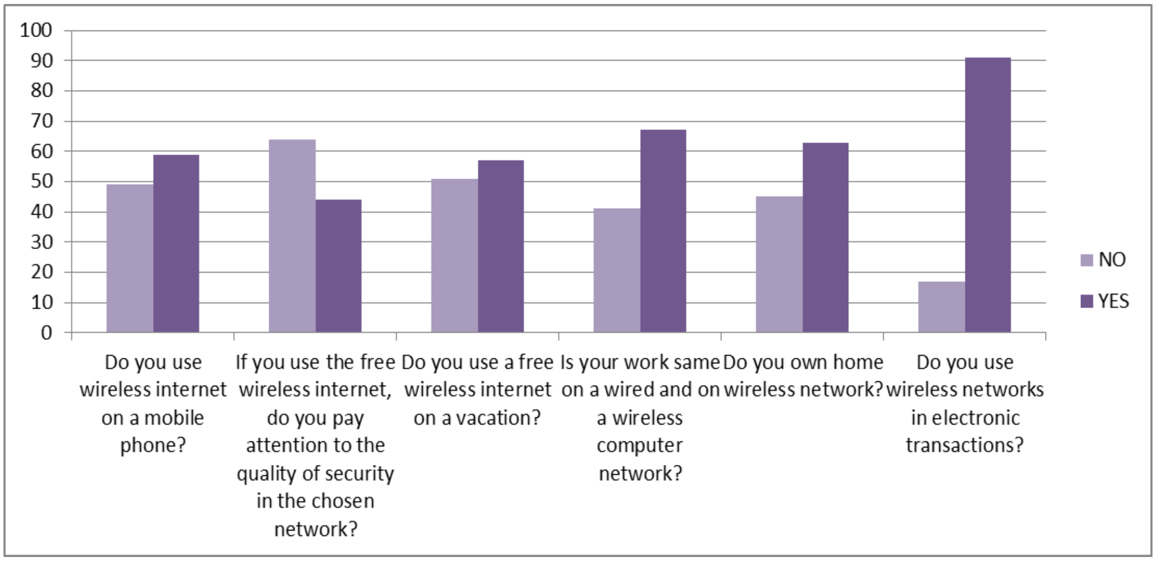
As the illustration shows, it is extremely difficult to notice the difference between the right-hand and left-hand screen. Except for the visual difference in only one letter, working client will not notice any difference in terms of work conditions. All the functionalities as seen by the client will remain at the same level while the pace of page loading will be almost identical in both cases. Therefore, this type of attack is difficult to notice and anticipate accordingly.

Presented attack is particularly interesting as seen on wireless networks, since the attacker does not need to have physical access to the local network but he can be at any location within the range of wireless network station. As the analysis obtained by the survey and presented in the upcoming paper segment has shown, most of the clients do not differentiate working within wired or wireless computer network. The analysis has also shown that most of the clients do not pay attention if the traffic within wireless computer network is encrypted, which additionally facilitates attempts of potential attackers (Adamovic 2011, Stephen 2010).

ANALYSIS OF THE DATA COLLECTED UPON HELD CONSULTATIONS

Based on presented analyses and tests we have conducted educational lecturing's and trainings including more than 150 participants. Group participants included final university year students as well as businessmen.

We have had two seminars in May 2011 – one in the territory of Republic of Serbia while the other was in the territory of Bosnia and Herzegovina. Consolidated survey data which the participants filled in are presented in the following picture.



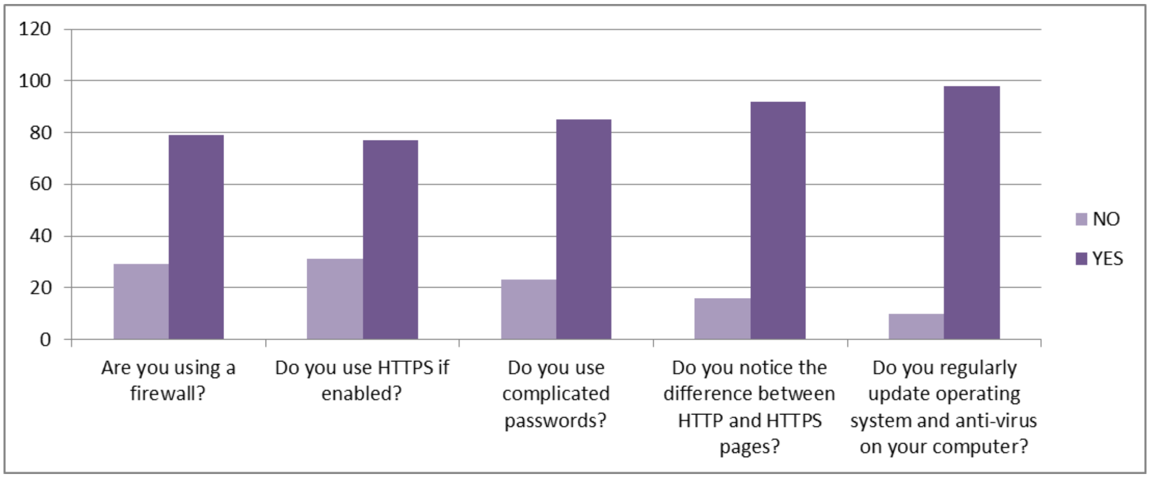
Picture No 8: Outcome of the survey held during one-day seminars

Survey of seminar participants has proved what had been presented in the introductory part of this paper. More than 90 % of the participants responded that they use wireless computer networks for the electronic transactions. Over 65% of the participants have at their possession household wireless computer networks and they do not differentiate working within wired or wireless computer network. What was underlined in this paper and its analyses is a safety factor which makes users of wireless computer networks specially vulnerable. It is true that attacks to SSL being presented in the work with wired computer network are feasible, but the identity of the attacker and existence of the attack is much more difficult to be detected with wireless computer network. Survey research has shown that ca 60% of the respondents use free Internet services during their holidays, and as per many analyses this is the most frequent period of time when the attacks occur. Analysis has further shown that over 60% of respondents will not pay attention to the use of unknown wireless computer network, which can make them particularly vulnerable to the attacks and data compromising.

It was determined through the seminars that over 65% of seminar participants own household wireless computer networks and that 50% of them have independently conducted configuration of the same. However, the most defeating fact was that 44% of the participants who have independently configured their networks have also opted not to protect the same from potential attacks.

As it was previously discussed and presented through the practical analysis in the previous paper work of the author called: Analysis of the wireless network security IEEE 802.11 - The city of Belgrade (Adamovic 2011). WEP presents old-fashioned protection mechanism which does not offer sufficient level of protection and which can be easily compromised.

Positive impression of the survey analysis was expressed in the fact that only 11% of respondents use old-fashioned and obsolete WEP mechanism which offers false sense of security.



Picture No 9: The application of security measures by users

Aim of the consultations was to change mentioned situation and raise awareness of the participants on the need of having protection of local wired and wireless computer networks upon use of e-business. During consultations we have carried out some of the practical methods of attack demonstrating, therefore the participants could see for themselves how some of the methods which they considered fully secure can be subject to compromising. Furthermore, we have significantly raised awareness on the need of use of cryptic mechanisms in working with wireless computer networks.

After analyzing response information gathered through questionnaire, we will proceed to drawing a conclusion about the proportion of well-informed and experienced wireless networks users among them. Based on our foreknowledge about educational level of participants, we expect the cohort of experienced and well-informed user of wireless networks to be the majority.

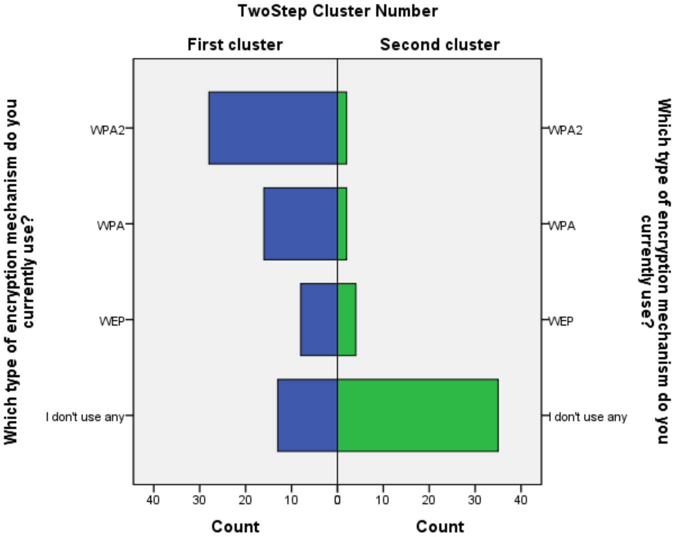
Table No 01: Questionnaire representation divided in clusters

		TwoStep Cluster Number	
		First cluster	Second cluster
		Column Total N %	Column Total N %
Did you set up your own Wi-Fi network at home?	No	23.1%	93.0%
	Yes	76.9%	7.0%
Do you use any of encryption mechanisms?	No	32.3%	95.3%
	Yes	67.7%	4.7%
Which type of encryption mechanism do you currently use?	I don't use any	20.0%	81.4%
	WEP	12.3%	9.3%
	WPA	24.6%	4.7%
	WPA2	43.1%	4.7%
Do you use HTTPS if it is enabled?	No	9.2%	58.1%
	Yes	90.8%	41.9%
Do you use Wi-Fi networks?	No	1.5%	37.2%
	Yes	98.5%	62.8%
Are you concerned about security while using Wi-Fi networks?	No	26.2%	69.8%
	Yes	73.8%	30.2%
Do you have a Wi-Fi network at your home?	No	26.2%	65.1%
	Yes	73.8%	34.9%
Do you make a distinction between HTTP and HTTPS web pages?	No	6.2%	27.9%
	Yes	93.8%	72.1%
Do you use a Firewall?	No	18.5%	39.5%
	Yes	81.5%	60.5%
If you use free of charge Wi-Fi networks while on vacation, are you concerned with their security level?	No	50.8%	72.1%
	Yes	49.2%	27.9%
Do you use free of charge Wi-Fi networks while on vacation?	No	41.5%	55.8%
	Yes	58.5%	44.2%
Do you use complex passwords?	No	16.9%	27.9%
	Yes	83.1%	72.1%
Do you use Wi-Fi networks on your cell phone?	No	41.5%	51.2%
	Yes	58.5%	48.8%
Is this lecture going to affect your usage of free of charge Wi-Fi networks in the future?	No	1.5%	2.3%
	Yes	98.5%	97.7%
Do you work in the same manner on both Wi-Fi and Wired networks?	No	38.5%	37.2%
	Yes	61.5%	62.8%
Do you update operating system and antivirus software on your computer regularly?	No	9.2%	9.3%
	Yes	90.8%	90.7%

In preference to scoring the results based on hypothetical model, we have performed a cluster analysis in order to identify participant's characteristics that are most relevant for differentiating the field of wireless networks security. We divide participants into two clusters, using SPSS Two-step Cluster method. The Schwarz's Bayesian information criterion was used to determine number of clusters, and the log-likelihood was used as measure of distance.

First cluster, with 65 members (60.19% of total) assigned to it is regarded to be comprised of less informed and less knowledgeable participants, while second cluster, with 43 members (39.81%) is considered to consist of informed participants.
Cluster analysis revealed that fact that security-aware wireless networks users tend to set up their own Wi-Fi networks at home, use WPA2 encryption mechanism, and HTTPS protocol when available, while updating operating system and antivirus software regularly, usage of Wi-Fi networks on cell phones and complex passwords do not seem

to be distinctive characteristics of them recently.



Picture No 10: Two-step Cluster method. The Schwarz’s Bayesian information criterion

CONCLUSION

Reduction of risk in electronic business running presents a complex procedure which consist of new technologies, organizational policies and procedures, new laws and industrial standards based on which state authorities can be authorized to pursue and punish committers of cyber-criminal acts. Problem of being safe while working on both wired and wireless computer networks in e-business is definitely present. Goal of this paper and organized seminars was to make wider audience aware of the problem existence. So as H1 presented lack of assurance is present, and H1 is proven to be true. However as H2 proposed interaction of users, hardware, and software is absolutely necessary and the problem must not be ignored. Through this paper we have presented that even the biggest systems, which vast majority considers fully safe for use, have certain shortcomings which ill-intentioned users can misuse. From the situation that the attacks were performed solely by those rare individuals who were well-thought and theoretically knowledgeable we outgrew to the situation that present tools for penetration tests do not require overly informed user. These tools which are primarily dedicated to penetration testing and diagnosis of computer networks can be also used by ill-intentioned individuals for their own personal benefits. Due to all aforementioned, paper authors consider of utter importance the topic on safety and raising awareness on the omissions which may be malevolently used.

It is beyond dispute that electronic business running has brought many benefits but also great dangers. The greater its development and use, the heavier the consequences of its misuse are.

Methodology that was used trough this paper shod be helpful as H3 presumes, and should be able to point out poetical fraud so users can take necessary steps to protect themselves. In the countries where this form of business running can be found in the constant expansion, many activities are undertaken in the safety field but also in the area of pursuing and punishing of those who started to perform misuses as their vocations.

This paper, lecturing’s and surveys are supported by the Ministry of Science and Technological Development of Republic of Serbia through the projects III44006, TR32054 – Digital processing within the system synthesis for information protection.

REFERENCES

Adamovic, S., Sarac, M., Radovanovic, D., (2011), Analysis of the wireless network security IEEE 802.11 - The city of Belgrade, Infotech, Jahorina

Alan Holt and Chi-Yu Huang, (2010), 802.11 Wireless Networks: Security and Analysis, Computer Communications and Networks

Amtul Fatima, (2009), E-Banking Security Issues – Is There A Solution in Biometrics?, Scholar, Jawaharlal University of Technological studies, A.P., India

Diana Widjaja, (2010), E-commerce Security, Encryption Methods for secure e-commerce websites, Carnegie Mellon University

Dierks, T., Allen, C., (1999), The TLS Protocl, IETF RFC 2246; online: www.ietf.org/rfc/rfc2246.txt.

Egwali Annie Oghenerukeybe, (2009), Customers Perception of Security Indicators in Online Banking Sites in Nigeria, Journal of Internet Banking and Commerce, April 2009, vol. 14, no.1 (http://www.arraydev.com/commerce/jibc/)

Howard, M., (2009), Man-in-the-Middle Attack to the HTTPS Protocol, IEEE computer society, p.78-81.

Muhammed S. Alnsour, Khalil Al-Hyar, (2011). Internet Banking and Jordanian Corporate Customers: Issues of Security and Trust, Journal of Internet Banking and Commerce, April 2011, vol. 16, no.1 (http://www.arraydev.com/commerce/jibc/)

Narciso Cerpa, Rodger Jamieson, (2009), A Security, Trust and Assurance Research Framework for Electronic Commerce, University of New South Wales, Sydney Australia NSW 2052

Ponemon Institute, (2011), Research Report, Cost of Cyber Crime Study, online: http://www.ponemon.org/local/upload/file/2011_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Radojevic, T., Radovanovic, D., (2010), The impact of electronic banking on offer of financial services, MIPRO 2010 Proceedings of the 33rd International Convention, Croatia

Robert L. Probert, Victor Sawma, (2003), Raising Awareness of Issues by Adapting the NIST IT Security Services Model to E-Business Systems, School of Information Technology and Engineering, University of Ottawa, http://csrc.nist.gov/organizations/fissea/2003-conference/presentations/sawna.pdf

Stephen E. Fienberg, (2010), Statistical methods in e-commerce research, Department of Statistics, Machine Learning Department, and Cylab Carnegie Mellon University, Pittsburgh PA 15213-3890, USA

Thomas, S., (2004), SSL and TLS Essentials, Wiley Computing Publishing, New York