ISSN 1330-3651
UDC/UDK 004.773.3.056

A COMPARATIVE STUDY OF THE SECURITY LEVEL AMONG DIFFERENT KINDS OF E-MAIL SERVICES – PILOT STUDY

Krešimir Šolić, Krešimir Grgić, Dario Galić

Preliminary notes

Free web-based e-mail services (e.g. gmail, yahoo and hotmail) are world-wide known and used among e-mail users for both personal and professional communication. However, because of the possible low security level they should not be the first choice when choosing an e-mail address. The objective of this study was to repeat the test applied on the world-wide known free web-based e-mail services and apply it on the institutional and ISP's e-mail services in the Republic of Croatia. The aim was to compare the security level of the e-mail services between free and non-free (professional) ones. The security test from earlier studies was applied on several e-mail addresses from each group by using session hijacking hacking tool to compare their security level. From nine e-mail services based in the Republic of Croatia only one was partly opened and that address was the only really free one. Comparison of these results with the earlier study, where the same test was applied on the top 10 free world-wide known web-based e-mail services, shows significant difference (p=0,034) regarding the level of security. The security test and comparison with previous testing has shown that it appears the free web-based e-mail services are less secure and therefore, whenever possible, should be avoided for professional usage.

Keywords: *e-mail, free web-mail services, security, web-based e-mail*

Usporedba stupnja sigurnosti među različitim vrstama e-mail servisa - pilot studija

Prethodno priopćenje

Besplatni web e-mail servisi (npr. gmail, yahoo, hotmail) se često koriste za profesionalnu korespondenciju, iako su lošijih sigurnosnih karakteristika od institucijskih e-mail adresa. U ovome istraživanju testiran je stupanj sigurnosti na institucijskim te e-mail servisima hrvatskih ISP-ova koje je prethodno provedeno na svjetski popularnim e-mail servisima. Cilj je bio usporediti stupanj sigurnosti među njima. Test se bazira na softverskom alatu koji preuzima sesiju web preglednika. Od devet e-mail servisa iz Hrvatske samo je jedan (ujedno i jedini stvarno besplatni servis) bio tek djelomično otvoren. Usporedbom s ranijim istraživanjem dobivena je statistički značajna razlika u korist hrvatskih e-mail servisa (p=0,034, Fisherov egzaktni test). Rezultati ovog istraživanja ukazuju na mogućnost da su svjetski poznati, besplatni, web bazirani e-mail servisi možda slabijih sigurnosnih karakteristika u usporedbi s institucijskim e-mail servisima u Hrvatskoj, te bi ih stoga trebali izbjegavati u profesionalnoj e-mail korespondenciji.

Ključne riječi: *e-mail, besplatni e-mail servisi, sigurnost, web e-mail servisi*

1
Introduction
Uvod

The e-mail service has become widely accepted and is being frequently used for both business and private communication. It represents a fast and convenient communication method which is at the same time disturbance-free for the recipient (the recipient autonomously chooses the moment when he will read the e-mail and answer it). In business environments the use of e-mail increases productivity and also reduces the communication costs. The use of e-mail for private communication is also much faster and more comfortable than the conventional mail service.

The e-mail service should comply with some basic security premises in order to satisfy the user's needs and requirements. It has to satisfy some basic security premises, such as [1]:

- authenticity
- confidentiality
- integrity
- non-repudiation.

The authenticity connotes that both sender and receiver are guaranteed their reciprocal identity. The confidentiality premise should ensure that, besides the sender and receiver involved in communication, nobody else can get the content of the message. The integrity premise ensures the protection against unauthorized modification of the message during transmission. The non-repudiation connotes that both sender and receiver are unable to deny the transmission of the message.

The security level of the used e-mail service primarily depends on the provider of the service. Currently, there are many web-mail services that are free of charge. Such services (e.g. gmail, yahoo and hotmail) have become very popular and are widely accepted and used. Unfortunately, certain researches proved some security weaknesses of these services.

The aim of this study was to repeat the test applied on the top world-wide known free web-based e-mail services and apply it to the institutional and ISP-s e-mail services in the Republic of Croatia. The aim was to compare the security level of e-mail services between the free and non-free ones (which in this case study means also comparison between .com and .hr domain) using session hijacking hacking test.

2
Session hijacking hacking test (tools and methods)
Hakerski test krađe sesije (alati i metode)

The most outspreaded hacking method for unauthorized access to mailboxes is the session hijacking method [5]. This intrusion method consists of several phases (Fig. 1). In the first phase the attacker has to capture network traffic which includes browser cookies and session ID exchanged between legal user and the mail server. After the attacker captures the victim's cookies he changes some values inside them. The attacker then substitutes his own cookies/session ID by the victim's cookies/session ID. In that way the attacker obtains the possibility to access the victim's e-mail account.

Online services (including web-based e-mail) that provide user access through web applications are also vulnerable to cross-site scripting attacks (XSS). Web applications use script code (JavaScript) that is embedded into web page to support dynamic client-side behaviour. This code is executed in the context of a user's web browser, which uses sand-boxing mechanism for limiting a script to access only resources related to its origin site. But this mechanism fails if the user downloads malicious script code from an intermediate (trusted) site. In that case the malicious script acquires access to all resources of the trusted site [4].

Web-based e-mail service has to employ a certain mechanism which enables the servers to recognize legal users and to differentiate them, since there is a possibility that many users are accessing their mailboxes at the same time. The server assigns a session ID to each successfully logged user. There are several possibilities for exchanging the session ID between the user's web browser and the mail server. The first possibility is to send the session ID together with the URL. This is not considered as a safe method, since the session ID is visible on the user's screen in the browser's address bar. The other possibility is to send the session ID together with the hidden field. This method provides a higher level of security, but the session ID can also be found by some available hacking tools.

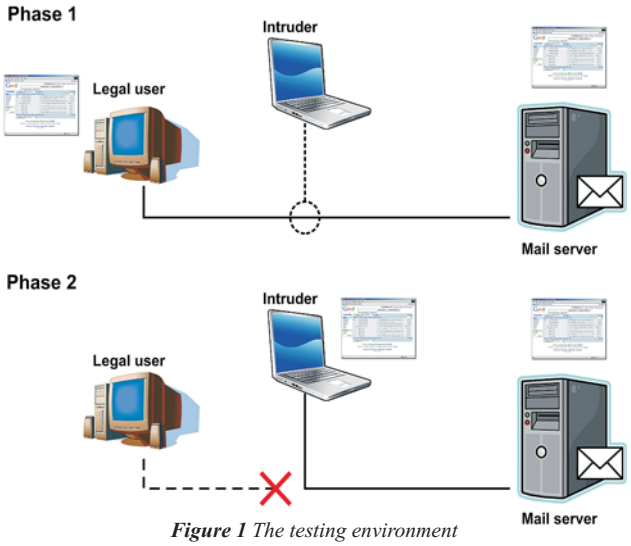

Figure 1 *The testing environment*
Slika 2. *Okruženje testiranja*

The most frequently used method (used by web-mail servers) is sending the session ID inside the web browser cookies. The most efficient method used by the attacker to get the legal user's session ID is called session hijacking. The session hijacking method has two main variants: hijacking by imitating one cookie and hijacking by copying all cookies (sidejacking).

During the first phase of attack the attacker sniffs the network traffic exchanged between the legal user and the web-mail server in order to get the packet containing the HTTP request. Afterwards the attacker extracts the cookies and finds the cookie containing the session ID. After discovering the session ID the attacker uses it as the substitution for his session ID in order to represent himself as the legal user to the web-mail server (he "hijacks" the session from the legal user). This method of attack is inefficient if the web-server constantly changes the session IDs, or the session ID is divided into several parts and stored in several cookies. In that case the attacker will use the sidejacking method (session hijacking by copying all cookies). By sniffing the victim's network traffic the attacker captures the whole HTTP Request (including cookies, URL and parameters). There are some available sidejacking hacking tools that are capable of repeating such HTTP Request in order to get the victim's HTTP Response. Afterwards, the used Sidejacking tool takes over further links and enables the attacker to obtain full control over the victim's mailbox [13]. The attacker is capable to read the victim's e-mails, and even to create and send new messages by misusing the victim's identity.

3
Results
Rezultati

The authors performed the session hijacking, sidejacking and XSS methods in order to test the security of different kinds of e-mail accounts. The test was first applied on the three most popular free world-wide used e-mail services, and the results were the same as in the previous study [2]:

- web-based e-mail with highest security level was Yahoo,
- the second one was Hotmail,
- with lowest security level was Gmail.

The positive fact is a constant provider's tendency for improving security of their services. For example, Gmail has recently improved its security by forcing users to use HTTPS (Hypertext Transfer Protocol Secure). The default option in Gmail is currently HTTP ('Always use https' in 'Browser Connection' settings), while previously the default option used to be HTTP. The HTTPS is a secure protocol which combines HTTP (Hypertext Transfer Protocol) with SSL/TLS (Secure Sockets Layer/Transport Layer Security) providing authenticated and encrypted communication.

The test was then applied to the nine e-mail addresses whose providers and institutions are based in the Republic of Croatia. There was one e-mail address that was partly opened and it is the only really free e-mail service among them (and in the Republic of Croatia). All the other e-mail services were secured regarding the applied test (Tab.1).

The difference is evident, even though the Fisher's Exact Test did not determine statistical significance (p=0,127) for the first set of data, probably because of the small sample.

Table 1 *Summarized results of the tested e-mail addresses regarding the level of security*
Tablica 1. *Zbirni rezultati testiranih e-mail adresa u pogledu razine sigurnosti*

Level of security	Free e-mail services	ISP's e-mail services	Institutional addresses
Totally opened	1	0	0
Partly opened	1	1	0
Secured e-mail addresses	1	3	5
Total	3	4	5
p=0,127, Fisher's Exact Test			

The comparison between the results found in this study and in the earlier study, where the same test was applied on the top 10 free world-wide known web-based e-mail services [5], shows a significant difference (p=0,034, Fisher's Exact Test) comparing the level of security (Tab. 2).

The Fisher's Exact Test was the chosen statistical test for determination of the significant differences between categorical data, because in some categories absolute frequencies were equal to zero.

Table 2 *Comparison of the tested e-mail addresses with reference study*
Tablica 2. *Usporedba testiranih e-mail adresa s pozivom na studiju*

	World-wide vice Croatian e-mail services/ No*	
Level of security	World top 10 free e-mail addresses**	E-mail addresses in Croatia
Totally opened	3	0
Partly opened	4	1
Secured e-mail addresses	3	8
Total	10	9
*p=0,034, Fisher's Exact Test **According to the previous study three groups were defined based on security level [5]		

4
List of possible security issues regarding e-mail system
Popis mogućih sigurnosnih pitanja u vezi e-mail sustava

E-mail system is dynamic and ever-developing part of the ICT system. This is a list of most of the security issues of that system that are known today, proposed by the authors of this manuscript consulting accessible literature and forum of the colleges ICT administrators [7, 11, 12]. This check-list is from users' perspective, so there are no parts of the e-mail system that are under the ISP's control. The list is as follows:

- using unsecured PC for accessing web-based e-mail (e.g. public PC, no antivirus and antispam protection installed)
- using less secure web browser (e.g. old version)
- not encrypting sensitive e-mails
- using web-browser when secure e-mail client is available
- opening executable or strange attachments
- not being critical to the unknown senders (opening e-mail from strange sender)
- replying to the strange/fake e-mails (phishing)
- sending personal and sensitive data by e-mail
- forwarding chain letters with list of all e-mail addresses included
- registering on the questionable/insecure web sites
- leaving its e-mail address to be known in public for everyone
- taking no care for its authentication data (e.g. revealing them to the friend in need)
- using less secure e-mail service provider
- using free world-wide known e-mail services when institutional one is available
- using insecure e-mail address for professional communication.

This is never-ending list that needs everyday updating and can be used as the check-list or the evaluation of the existing e-mail system in order to find critical or less secure parts.

5
Conclusion
Zaključak

Because the p values were small (close to and smaller than 0,05) for both comparisons this research shows that it might be that world-wide known free e-mail services are less secured than the institutional ones.

One reason might be that the institutional e-mail services have significantly less users than the world-wide available free e-mail services. Therefore, they are probably less exposed to different attack attempts.

Apart from looking much more professional when using institutional e-mail service, security issues regarding particular institutional e-mail service are under control: e-mail server with user's data is usually physically within the institution.

In the previous study increasing trend was found in the usage of the world-wide known free e-mail services among researchers in biomedical fields [8]. And in the other one it was shown that there is no significant difference regarding the knowledge on security issues, between the researchers with biomedical or technical background knowledge [3]. According to those studies it seems that even high educated people are not aware of the security issues of the e-mail services.

Some users maybe choose free e-mail addresses rather than the institutional ones because they do not have web-based or even any kind of e-mail server at their institution, and for them it can be the only choice. However, in general, all e-mail users should be aware that the insecure e-mail services are not a good choice for everyday professional communication.

One possible limitation of this study may be in a small number of e-mail addresses compared. Also the test on top 10 free world-wide known e-mail services was done earlier and the security level of some of those e-mail services could have become better at the time of this research. Nevertheless, there are many other reasons for e-mail user to prefer institutional e-mail address for professional electronic communication.

The results of this pilot study can be a starting point for the future research on security issues regarding e-mail communication as part of the ICT systems and for testing just how much more spam and viruses are coming through free e-mail services versus not so widely used institutional e-mail addresses.

6
References
Literatura

[1] Min-Hua Shao, Guilin Wang, Jianying Zhou. Some common attacks against certified email protocols and the countermeasures, Computer Communications, 29 (2006), p. 2759-2769.
[2] Chomsiri, T. A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test. // IJCSNS, 8, 5(2008), p. 23-26.
[3] Solic, K.; Ilakovac, V. Security Perception of a Portable PC User (The Difference Between Medical Doctors and

Engineers): A Pilot Study // Medicinski glasnik Ljekarske komore Zeničko-dobojskog kantona, 6, 2 (2009), p. 261-264.
[4] Kirda, E.; Jovanovic, N.; Kruegel, C.; Vigna, G. Client-side cross-site scripting protection // Computers & Security, 28, (2009).
[5] Noiumkar, P.; Chomsiri, T. Top 10 Free Web-Mail Security Test Using Session Hijacking. // IEEE CS ICCIT '08 / uredili P.P. Wang, S. Sohn, G. Dhillon, J. Lee, F.I.S. Ko, N.T. Nquyen, J. Bi, K. Sakurai, et al. 2008, 2, p. 486-490.
[6] Solic K.; Grgic, K. Usage of Unsecured Free Web-based E-mail Services among Biomedical Researchers. // IEEE 31st ITI '09 /uredili Vesna Luzar-Stiffler, Iva Jarec, Zoran Bekic, 2009, poster.
[7] Silic, M.; Krolo, J.; Delac, G. Security Vulnerabilities in Modern Web Browser Architecture. // IEEE, 33th international conference MIPRO / V. Mornar, P. Biljanović, J. Kljajić, I. Škunca, 2010, p. 33.
[8] Solic, K.; Ilakovac, V.; Marusic, A.; Marusic, M. Trends in using insecure e-mail services in communication with journal editors. // 6th Peer Review and Biomedical Publication / uredili D. Rennie, A. Flanagin, F. Godlee, J. Smith, 2009, str. 50.
[9] Arrington, M. Gmail Disaster: Reports Of Mass Email Deletions. // TechChrunch. The Web version (2006), http://www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/ (20.01.2009.).
[10] Stewart, J. Private Email Accounts Go Public Watch. // Death By Email. The Web version (2007), http://www.deathbyemail.com/2007/08/private-email-a.html (20.01.2009.).
[11] The 25 Most Common Mistakes in Email Security. // ITSecurity. The Web version (2007), http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/ (20.01.2009.).
[12] Top 5 Ways to protect your Email. // ITSecurity. The Web version (2007), http://www.itsecurity.com/whitepaper/five-essential-steps-to-safer-email-ironport/index.php (20.01.2009.).
[13] Web source for SideJacking Tool. // ErrataSec. 2008. http://www.erratasec.com/sidejacking.zip (25.08.2008.).

Authors' addresses
Adrese autora

Krešimir Šolić, dipl. ing.
Department of Biophysics
Medical Statistics and Medical Informatics
Faculty of Medicine
J. J. Strossmayer University of Osijek,
Josipa Huttlera 4
HR-31000 Osijek, Croatia
kresimir@mefos.hr

Krešimir Grgić, dipl. ing.
Department of Communications
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
K. Trpimira 2b
HR-31000 Osijek, Croatia
kresimir.grgic@etfos.hr

Mr. sc. Dario Galić, prof.
Department of Biophysics
Medical Statistics and Medical Informatics
Faculty of Medicine
J. J. Strossmayer University of Osijek
Josipa Huttlera 4
HR-31000 Osijek, Croatia
galic@mefos.hr