NETWORK PERIMETER SECURITY FOR MEDICAL INFORMATION SYSTEMS

Tzveta Dimitrova

Faculty of Telecommunication, Technical University - Sofia,8, “Kliment Ohridsky” str., 1000 Sofia,Bulgaria,
E-mail: tz.dimitrova@gmail.com

Abstract

This study analyzed vulnerabilities in networked computer systems that are accessible from the internet. Vulnerabilities are defects, bugs or misconfigurations in software that can be exploited by an attacker to compromise the confidentiality, integrity or availability of information. Vulnerabilities in networked systems are a major source of today’s information security risks, as they expose an organization and its assets to external threats like black-hat hackers, crackers or plain criminals. New vulnerabilities are discovered every day. Thus, with the development of telemedicine, hospitals that rely on dependable information systems need to frequently assess their exposure to these vulnerabilities in order to be able to manage their risk. Today, vulnerability management is no longer just a technical need, it has become a legal requirement for many medical organizations that seek to fulfill modern compliance regulations and conduct business internationally. The article present the results of a recent vulnerability exposure assessment conducted in 32 different medical organizations. The results show the most vulnerable system types, service families and network ports. They further evaluated differences in the risk exposure of medical organizations with different kinds of vulnerability management practices such as regular automated vulnerability scans.

1. INTRODUCTION

The following analysis is based on the assessment of 523 Vulnerabilities on 42 hosts in 32 medical organizations. To protect the identity of the participating medical organizations and because the same standard software products like Apache web servers or PHP are used in all medical organizations regardless of their size, headcount or business area we have excluded that information from the assessment. The purpose of the analysis is not to provide statistical proof for particular claims, but to learn from examples to help better protect all medical organizations’ assets.

2. KEY FINDINGS:

High-risk vulnerabilities make up on third (33%) of the total number of identified vulnerabilities.

A large part of the analyzed medical organizations (47%) suffered from such high-risk6 vulnerabilities. However, 41% managed to have neither high nor medium-risk vulnerabilities. (Figure1)

Medical organizations that manage their vulnerability exposure through regular vulnerability scans or security audits show a tendency of reduced risk exposure compared to other medical organizations.

The most common vulnerability had an average CVSS severity score[1] of 5.86 (at a standard deviation of 1.79) and is found on a web server running PHP behind the ports 80 or 443.

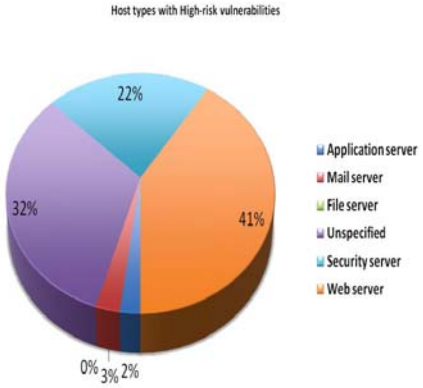

Fig. 1: The share of hosts that suffered from high-risk vulnerabilities - by host type.

3. RISK FACTORS OF VULNERABILITIES BY HOST TYPE[2]

The identified vulnerabilities were unevenly distributed among the analyzed host types. The largest share of high-risk vulnerabilities was found on web servers, followed by application and security servers. An explanation for the surprisingly high number of vulnerabilities on security servers, such for example firewalls, could be the fact that many of these security systems are themselves based on vulnerable

[1] The Common Vulnerability Scoring System (CVSS) measures the relative severity of a vulnerability on a scale from 0 (low) to 10 (high). CVSS is used by the National Vulnerability Database (NVD). Specification available online at http://www.first.org/cvss/

[2] The type of a server was determined by the it’s main use in the organization and not by its technical characteristics such as installed software. The main use was provided by the organization in a pre-study questionnaire.

platforms like Linux, Unix or provide user interfaces using insecure PHP/HTTP components. (Table 1)

Table 1: The share of host types that suffered from high-, medium- or low risk vulnerabilities

Host Type	*High*	*Medium*	*Low*	*Tota*
Application server	2%	1%	0%	1%
Mail server	3%	1%	0%	1%
File server	0%	0%	0%	0%
Unspecified	32%	80%	74%	71%
Security server	22%	8%	12%	10%
Web server	41%	10%	14%	16%
Total	100%	100%	100%	100%

4. VULNERABILITY FAMILIES

PHP vulnerabilities were overall the most common, followed by those related to the Apache web server and SSH, SSL. When only severe vulnerabilities (with a CVSS score >7) are taken into consideration however, the Apache vulnerabilities are almost insignificant whereas PHP weaknesses dominate the picture. (Figure 2). The common web ports 80 (HTTP) and 443 (HTTPS) lead in all risk categories. Most vulnerability that were found on the standard SSL port 22 were only of low risks. (Table 2).

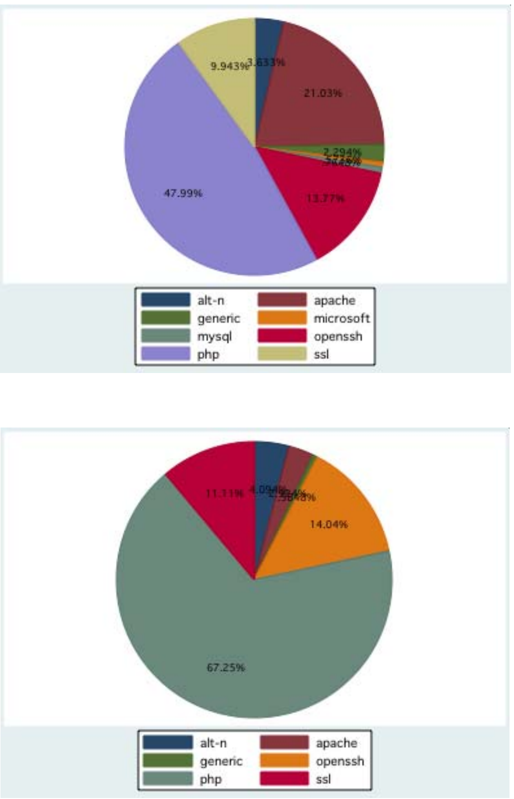

Fig. 2. Up - all vulnerabilities – Down: Vulnerabilities with CVSS score > 7

Table 2: Suffered from vulnerabilities with a risk factor of:

Port	*High*	*Medium*	*Low*	*Total*
21	0%	2%	0%	1%
22	9%	8%	26%	10%
25	0%	1%	0%	0%
80	58%	38%	34%	44%
110	4%	4%	5%	4%
443	19%	21%	8%	20%
445	1%	1%	3%	1%
465	1%	0%	0%	0%
587	0%	0%	0%	0%
666	1%	6%	3%	4%
822	5%	3%	11%	4%
995	1%	1%	0%	1%
3306	0%	1%	5%	1%
3389	0%	0%	0%	0%
4242	1%	6%	3%	4%
7600	1%	6%	3%	4%
8088	1%	1%	0%	1%
19638	1%	1%	0%	1%
Total	100%	100%	100%	100%

5. MEDICAL ORGANIZATIONS

A quarter (25%) of the analyzed medical organizations were evaluating their vulnerability exposure on a regular basis either through security audits (9%), automated (16%)- or manual vulnerability scans (19%). Medical organizations that did not conduct such evaluations showed a tendency towards larger numbers of high- and medium risk vulnerabilities on their hosts. (Figure 3).

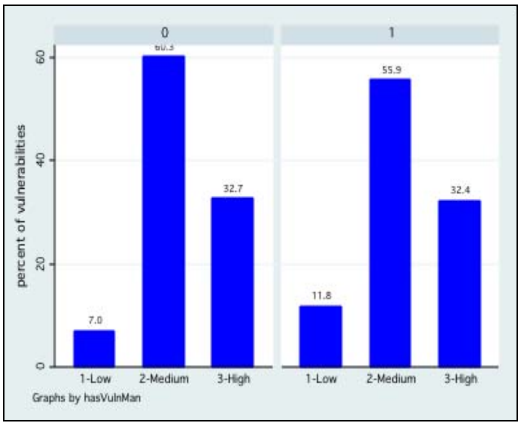

Fig. 3: Left: Medical organizations without vulnerability management activities. Right: Medical organizations conducting Security audits or automated or manual vulnerability scans.

Average vulnerability severity in medical organizations

A large part of the analyzed medical organizations (47%) suffered from high-risk vulnerabilities. However, 41% managed to have neither high nor medium-risk vulnerabilities. The average severity score across all identified vulnerabilities was 5.86 (with a standard deviation of 1.79). (Figure 4) (Table 3).

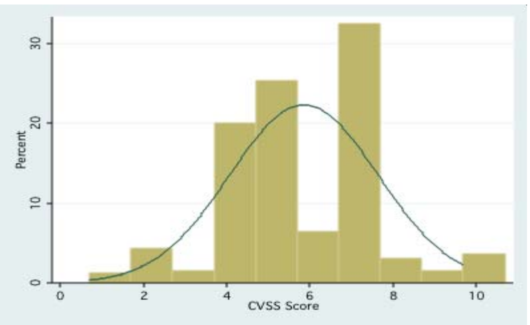

Fig. 4: Histogram of the CVSS scores of all identified vulnerabilities

Table 3: Suffered from 1 or more vulnerabilities with a risk factor of

Organization	*High*	*Medium*	*Low*
ID001	yes	yes	no
ID002	no	yes	no
ID003	yes	yes	yes
ID004	no	no	no
ID005	no	no	no
ID006	yes	yes	yes
ID007	no	no	no
ID008	no	no	no
ID009	yes	yes	yes
ID010	no	no	no
ID011	yes	yes	yes
ID012	no	no	yes
ID013	yes	yes	yes
ID014	no	yes	no
ID015	yes	yes	yes
ID016	no	yes	no
ID017	yes	yes	no
ID018	yes	yes	no
ID019	yes	yes	no
ID020	no	no	no
ID021	yes	yes	no
ID022	no	no	no
ID023	no	no	no
ID024	no	no	no
ID025	no	no	no
ID026	no	yes	no
ID027	yes	yes	no
ID028	yes	yes	no
ID029	yes	yes	no
ID030	no	no	no
ID031	yes	yes	yes
ID032	no	no	no

6. CONCLUSIONS

Among the participating medical organizations in this study, many showed a low level of vulnerability exposure and demonstrated that high-risk vulnerabilities are not inevitable. Based on their success, we suggest the following actions to be taken by organization managers and network administrators.

Network administrators

There are clear hot spots for vulnerabilities: Services related to web servers are among the most common sources for vulnerabilities. These systems are worthy extra attention and should be evaluated more regularly by administrators and their security staff.

All of the vulnerabilities identified in this study were found using automated vulnerability scanning tools that are publicly available. Administrators should make increasing use of the automated tools in order to be able to reduce their workload and conduct evaluations more frequently.

Organization Managers

Many of the found vulnerabilities had been publicly known for a long time. Establish an organizational process to find and react on new vulnerabilities in a timely manner.

As medical organizations change so do their Medical IT systems and their exposure to vulnerabilities. The more dynamic a network or a system becomes the more frequent vulnerability exposure assessments should be carried out.

References

[1] O. Jones, M. Thompson, and J.K. Nielsen, *Book Title*, Publisher, Location, Date.

[2] Anderson, R., “Why information security is hard - an economic perspective”. 17th Annual Computer Security Applications Conference. ACSAC. Proceedings (2001)

[3] Blount, Summer. “The role of security management in achieving continuous compliance”, Whitepaper: Compliance, CA Security Management, October 2006

[4] Brenner, M. Classifying ITIL Processes; A Taxonomy under Tool Support Aspects. Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on, (2006), 19-28.

[5] Chen, Y. Stakeholder Value Driven Threat Modeling for Off The Shelf Based Systems. International Conference on Software Engineering, IEEE Computer Society Washington, DC, USA (2007), 91-92.

[6] Frühwirth Christian. "On Business-Driven IT Security Management and Mismatches between Security Requirements in Firms, Industry Standards and Research Work". PROFES 2009: pp. 375-385 (2009)

[7] L. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. ACM Transactions on Computer Human

[8] Interaction, 12(2):135–178, 2006.

[9] R. de Paula and et. al. Two experiences designing for effective security. In SOUPS '05: Proceedings of the second symposium on Usable privacy and security, New York, NY.

[10] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

[11] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In SOUPS '06: Proceedings of the second symposium on Usable privacy and Security, New York, NY, USA, 2006. ACM.

[12] D. Florencio and B. C. Cormac Herley. Do strong web passwords accomplish anything? In Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec), 2007.

The author wish to thank the European Commission for the grant in the Lifelong Learning Programme, the Executive Agency for its help and all the partners of the project for their contribution.
Project Number: 142814-LLP-1-2008-FR-ERASMUS-ENW
Instrument type: ERASMUS NETWOR