Web Security: Cyber Crime Perspective

Divyanshi Garg[1], Anand Sharma[2]
[1,2]CET-MUST, Lakshmangarh
[1]*divyanshigarg060@gmail.com*, [2]*anand_glee@yahoo.co.in*

Abstract: Websites of organizations face more security threats than ever before. Web security is the biggest problem in the digitally connected world. Cyber-criminals are on the lookout for probable vulnerability in websites. They target the users via the sites users visit. The web security is the outcome of broad security valuation of the present circumstances on the web. Website hosts, Content Management Systems and anti-virus suites constantly update to provide protection from the latest threats. This paper discusses web security policies in the context of requirements for network security and the circumstances in which those requirements must be encountered, examines common methods of threat control, and reviews system vulnerabilities, in mandate to motivate reflection of the specific sorts of web security mechanisms that can be built into networks.

*****

I. Web Security

The Web security platform guide identifies assets in the web infrastructure (i.e., the client and server machines), assets in the application (such as client-side application code and serverside application storage) and user-related assets (such as authentication credentials and personal information)

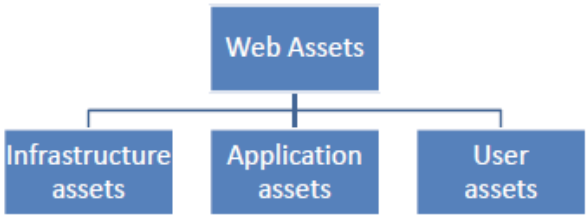

Fig 1: Assets in the web infrastructure, assets in the application, and user-related assets

For each asset, we discuss its importance and the attacker's incentives for compromising this asset, and analyze how an asset can be compromised. In order to structure the variety of ways available to compromise an asset, we use trees to explicitly define high-level threats against an asset. These threats are intermediate steps that an attacker has to take in order to compromise an asset, and are typically common across different assets.

II. Attacks on the Web Platform

web security vulnerability landscape is constructed, by investigating how an attacker can execute the threats to compromise an asset. To do so, the threats identified are grouped together in seven high-level threat categories:

1) Impersonating users
2) Forging requests
3) Attacking through the network
4) Controlling the client-side context
5) Attacking the client-side infrastructure
6) Directly attacking the web application
7) Violating the user's privacy

For each of the seven high-level threats, the most representative attack techniques have been selected, and are reported in more detail.

Three top web site vulnerabilities for Cyber Crimes

SQL Injection

- Browser sends malicious input to server
- Bad input checking leads to malicious SQL query

CSRF – Cross-site request forgery

- Bad web site sends browser request to good web site, using credentials of an innocent victim

XSS – Cross-site scripting

- Bad web site sends innocent victim a script that steals information from an honest web site

III. Dealing with Cyber Crimes for web site vulnerabilities

Preventing SQL Injection

- Never build SQL commands yourself !
  - Use parameterized/prepared SQL
  - Use ORM framework

CSRF Defenses

- Secret Validation Token
- Referer Validation
- Custom HTTP Header

Protection Against XSS – Cross-site scripting

- Validation of all headers, cookies, query strings, form fields, and hidden fields
- Never attempt to identify active content and remove, filter, or sanitize it.
- 'Positive' security policy that specifies what is allowed.

IV. Conclusion

In this paper we have presented Web services, an emerging technology for the Web, The web service overviewand the various security issues occurred in the implementation. Thesecurity of web services is an important aspect and hence a security mechanism is required to implement in webservices for key generation and encryption decryption of the messages.This paper discussed web security policies in the context of requirements for network security and the circumstances in which those requirements must be encountered, examines common methods of threat control, and reviews system vulnerabilities, in mandate to motivate reflection of the specific sorts of web security mechanisms that can be built into networks to protect from cyber criminals.

References

[1] Monika Sachdeva, Krishan Kumar Gurvinder Singh Kuldip Singh SBS College of Engg. & Technology, Guru Nanak Dev University Indian Institute of Technology Ferozepur, Punjab, India Amritsar, Punjab, India Roorkee, Uttarakhand, Indiamonika.sal(kediffmail.com gzsbawa7 1(yahoo.om kds56fec(&riitr.ernetmin) Performance Analysis of Web Service under DDoS Attacks 2009 IEEE International Advance Computing Conference (IACC 2009)Patiala, India, 6-7 March 2009

[2] Adam Kie˙zun MIT akiezun@csail.mit.edu Philip J. Guo Stanford University pg@cs.stanford.edu KarthickJayaraman Syracuse University kjayaram@syr.edu Michael D. Ernst University of Washingtonmernst@cs.washington.edu

[3] E. Kirda, C. Kruegel, G. Vigna, and N. Jovanovic, “Noxes: A clientside solution for mitigating crosssite scripting attacks,” in Proceedingsof the 12th ACM Symposium on Applied Computing, 2006.

[4] T. Gallagher, “Automated detection of cross site scripting vulnerabilities,” European Patent Application EP1420562 (pending), October 2003.

[5] Liang Guangmin Computer Engineering Department Shenzhen Polytechnic, Shenzhen 518055, China Email: gmliang@oa.szpt.net Third 2008 International Conference on Convergence and Hybrid Information Technology Modeling Unknown Web Attacks in Network Anomaly Detection.

[6] DraganVidakovicGimnazijaIvanjica vidakd@ptt.yu DejanSimic FON Belgrade dsimic@fon.bg.ac.yu A Novel Approach to Building Secure Systems

[7] Open Web Application Security Project. The ten most critical Web application security vulnerabilities. http://umn.dl.sourceforge.net/ sourceforge/owasp/OWASPTopTen2004.pdf, 2004, visit on 2005/10/05

[8] Jin-Cherng Lin and Jan-Min Chen, “An Automatic Revised Tool for Anti-malicious Injection”, in Proceedings of The Sixth IEEE International Conference on Computer and Information Technology .

[9] Igino Corona, DavideAriu and Giorgio Giacinto This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings HMM-Web: a framework for the detection of attacks against Web applications.

[10] C. Criscione, G. Salvaneschi, F. Maggi, S. ZaneroDipartimento di Elettronica e Informazione — Politecnico di Milano 2009 European Conference on Computer Network Defense Integrated Detection of Attacks Against Browsers,Web Applications and Databases.

[11] Vipul Patel, Radhesh Mohandas and Alwyn R. Pais Information Security Research Lab, National Institute of Technology Karnataka, Surathkal, India {vip04pat, radhesh, alwyn.pais}@gmail.com
ATTACKS ON WEB SERVICES AND MITIGATION SCHEMES.