Estimating Security Risk for Web Applications using Security Vectors

Hui Guan[1, 3, *], Wei-Ru Chen[1], Lin Liu[2], and Hong-Ji Yang[3]

[1] School of Computer Science and Technology,
Shenyang University of Chemical Technology,
Shenyang , China
guanh1999@126.com, willc@china.com

[2] School of Software,
Tsinghua University,
Beijing, China
linliu@tsinghua.edu.cn

[3] Software Technology Research Laboratory,
De Montfort University,
Leicester, England
hyang@dmu.ac.uk

Received 18 September 2011; Revised 12 January 2012; Accepted 15 February 2012

Abstract. Risk assessment has been getting increased attention as the new vulnerabilities and threats are emerging on daily basis. The popularity and complexity of web application present challenges to the security implementation for web engineering. It is well known that the earlier to perform risk assessment for software, the less cost needed to mitigate the security risks. However, quantitative estimation of security in the earlier stage of software development life cycle is largely missing. In this paper, we propose a quantitative approach to perform risk assessment at design stage for web application which is based on multiple security vectors of asset, threat and vulnerability. An environment-driven method is proposed to elicit threats to the system. In the end, the risk assessment methodology is applied on a customer goods case study.

Keywords: risk assessment; threat; security; asset; vulnerability; design stage

Acknowledgment

This work was sponsored by Liaoning Province Office of Education of China Project Research on Security-oriented Software Reengineering (Grant No. L2010439) and partial financial support by the National Natural Science Foundation of China (Grant No. 60873064 and Grant No. 90818026).

References

[1] B. D. R. Marino, H. M. Haddad, J. E. Molero A, "A Methodological Tool for Asset Identification in Web Applications," in *Proceeding of the 4th International Conference on Software Engineering Advances*, Porto, Portugal, pp. 413-418, 2009.

[2] Web Application Security Trends Report, http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf

[3] The Importance of Application Classification in Secure Application Development, http://www.webappsec.org/projects/articles/041607.shtml

[4] J. R. Maguire and H. G. Miller, "Web-application Security: From Reactive to Proactive," *IT Professional*, Vol. 12, No. 4, pp. 7-9, 2010.

*Correspondence author

[5] G. Sindre and A. L. Opdahl, "Eliciting Security Requirements with Misuse Cases," *Requirements Engineering*, Vol. 10, No. 1, pp. 34-44, 2005.

[6] I. F. Alexander, "Misuse Cases: Use Cases with Hostile Intent," *IEEE Software*, Vol. 20, No. 1, pp. 58-66, 2003.

[7] D. G. Firesmith, "Analyzing the Security Significance of System Requirements," in *Proceedings of Symposium on Requirements Engineering for Information Security*, Paris, France, 2005.

[8] F. A. Braz, E. B. Fernandez, M. VanHilst, "Eliciting Security Requirements through Misuse Activities," in *Proceeding of the 19th International Workshop on Database and Expert Systems Applications*, Turin, Italy, pp. 328-333, 2008.

[9] F. Swiderski and W. Snyder, Threat modeling, Microsoft Press, Redmond, Washington, 2004.

[10] I. A. Tondel, M. G. Jaatun, P. H. Meland, "Security Requirements for the Rest of Us: A Survey," *IEEE Software*, Vol.25, No. 1, pp. 20-27, 2008.

[11] S. Myagmar, A.J. Lee, W. Yurcik, "Threat Modeling as a Basis for Security Requirements," in *Proceeding of Symposium on Requirements Engineering for Information Security*, Paris, France, 2005.

[12] M. A. Hadavi, H. Shirazi, H. M. Sangchi, V. S. Hamishagi, "Software Security: A Vulnerability-activity Revisit," in *Proceeding of the 3rd International Conference on Availability, Reliability and Security*, Barcelona, Spain, pp. 866-872, 2008.

[13] J.D. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamilla, A. Murukan, Improving Web Application Security: Threats and Countermeasures, Microsoft Press, Redmond, Washington, 2003.

[14] C. Möckel and A. E. Abdallah, "Threat Modeling Approaches and Tools for Securing Architectural Designs of an E-banking Application," in *Proceeding of the 6th International Conference on Information Assurance and Security*, Atlanta, GA, USA, pp. 149-154, 2010.

[15] An Approach to Web Application Threat Modeling, http://www.infosecwriters.com/text_resources/pdf/AShrivastava_Web_Application_Threat_Modeling.pdf

[16] E. A. Oladimeji, S. Supakkul, L. Chung, "Security Threat Modeling and Analysis: A Goal-oriented Approach," in *Proceedings of the 10th International Conference on Software Engineering and Applications*, Dallas, Texas, USA, 2006.

[17] M. Jackson, "Problem Frames and Software Engineering," *Expert Systems*, Vol. 25, No. 1, pp. 7-8, 2008.

[18] C. B. Haley, R. C. Laney, J. D. Moffett, B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis," *IEEE Transaction On Software Engineering*, Vol. 34, No. 1, pp. 133–153, 2008.

[19] D. Hatebur, M. Heisel, H. Schmidt, "Analysis and Component-based Realization of Security Requirements," in *Proceedings of the 3rd International Conference on Availability, Reliability and Security*, Barcelona, Spain, pp. 195-203, 2008.

[20] J. P. Jesan, "Threat Modeling Web-applications Using STRIDE Average Model," in *Proceedings of Computer Security Conference*, Myrtle Beach, USA, 2008.

[21] Protecting Sensitive Compartmented Information within Information Systems, http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm

[22] L. Liu, E. S. K. Yu, J. Mylopoulos, "Secure-i*: Engineering Secure Software Systems through Social Analysis," *International Journal of Software and Informatics*, Vol. 3, No. 1, pp. 89-120, 2009.

[23] L. Liu, E. Yu, J. Mylopoulos, "Secure Design Based on Social Modeling," in *Proceedings of the 30th Annual International Computer Software and Applications Conference*, Chicago, IL, USA, pp. 71-78, 2006.

[24] T. Long, L. Liu, Y.J. Yu, Z. Jin, "AVT Vector: A Quantitative Security Requirements Evaluation Approach based on Assets, Vulnerabilities and Trustworthiness of Environment," in *Proceedings of the 17th IEEE International Requirements Engineering Conference*, Atlanta, Georgia, USA, pp. 377-378, 2009.

[25] H. Guan, W.R. Chen, L. Liu, H.J. Yang, "Environment-driven Threats Elicitation for Web Application", in *Proceeding of Agent and Multi-Agent Systems: Technologies and Applications*, Manchester, UK, Vol. 6682 , pp. 291-300, 2011.

[26] BSI, Code of Practice for Information Security Management, British Standards Institute, London, 1999.

[27] Y.J. Chung, I.J. Kim, N.H. Lee, T. Lee, H. P. In, "Security Risk Vector for Quantitative Asset Assessment," in *Proceeding of International Conference on Computational Science and Its Applications*, Singapore, Vol. 3481, pp. 274-283, 2005.

[28] D. Verdon and G. McGraw, "Risk Analysis in Software Design," *IEEE Security and Privacy*, Vol. 2, No. 4, pp.79-84, 2004.

[29] I. Mkpong-Ruffin, D. A. Umphress, J. Hamilton, J.Gilbert, "Quantitative Software Security Risk Assessment Model," in *Proceeding of the 3rd ACM Workshop on Quality of Protection*, Alexandria, VA, USA, pp.31-33, 2007.

[30] Risk Management Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[31] Methodology for Information Systems Risk Analysis and Management, https://www.ccn-cert.cni.es/publico/herramientas/pilar43/en/magerit/meth-en-v11.pdf

[32] A Complete Guide to the Common Vulnerability Scoring System Version 2.0, http://www.first.org/cvss/cvss-guide.html#i2.2.1

[33] OCTAVE, http://www.cert.org/octave/

[34] D. D. Cock, K. Wouters, D. Schellekens, D. Singelee, B. Preneel, "Threat Modelling for Security Tokens in Web Applications," in *Proceeding of the 8th Conference on Communication and Multimedia Security*, Windermere, UK, pp. 213-223, 2004.

[35] L. Jiang, H. Chen, F. Deng, "A Security Evaluation Method Based on STRIDE Model for Web Service," in *Proceeding of the 2nd International Workshop on Intelligent Systems and Applications*, Wuhan, China, pp. 1-5, 2010.

[36] Threat Risk Modeling, https://www.owasp.org/index.php/Threat_Risk_Modeling