Proceedings of the 13th International Conference on Quality and Dependability
Neptun, Romania, September 5th-7th, 2012
ISSN 1842-3566
Pages 200-206

Survivability Analysis Based on Attack Models

Ioan-Cosmin MIHAI, Angelica BACIVAROV, Ioan C. BACIVAROV

Police Academy, Faculty of Police, Bucharest, Romania; EUROQUALROM, Electronics, Telecommunications and Information Technology Faculty, University "Politehnica" of Bucharest, Romania; EUROQUALROM, Electronics, Telecommunications and Information Technology Faculty, University "Politehnica" of Bucharest, Romania
angelica@euroqual.pub.ro

Abstract
Survivability is the capability of a system to fulfill its mission in a timely manner despite intrusions, failures or accidents. This paper analyzes the concept of survivability and examines some models to ensure the virtual machines survivability. Possible attacks on a virtual machine are presented, too. The conclusion is that there is no "absolute" survivability on informatics systems. Some attack or other may compromise any system, however well defended. It is interested in assessing the strength of a current defense mechanism of a system of a given design relative to a stochastic incidents process. The actual survivability could be a function of many other factors such as the policies of the system managers, the "behavior" of the system and the deterrence it can induce among potential attackers, its reaction (detection, resistance, recovery), or the publicity surrounding an incident experienced by the system.

Keywords: attack model, attack tree, security, survivability, virtual machine

References:

[1] Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff and John McHugh; "Survivable Network Analysis", Pittsburgh, PA 15213-3890: Software Engineering Institute, Carnegie Mellon University, 2000;
[2] R. Ellison, D. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff and N. Mead, "Survivable Network Systems: An Emerging Discipline", Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999;
[3] Richard C Linger, Howard F. Lipson, John McHugh, Nancy R. Mead and Carol A. Sledge; "Life-Cycle Models for Survivable Systems", CMU/SEI-2002-TR-026, Networked Systems Survivability Program, Carnegie Mellon University, 2002;
[4] Andrew P. Moore, Robert J. Ellison and Richard Linger, "Attack Modeling for Information Security and Survivability", CMU/SEI-2001-TN-001, Technical Report, 2001;
[5] Fisher, D.A., "Emergent Algorithms–A New Method for Enhancing Survivability in Unbounded Systems", IEEE Proceedings of the Hawaii International Conference on Systems Sciences. Wailea, HI, Jan. 5-7, 1999;
[6] DISA, Department of Defense of United State of America, "Security Technical Implementation Guide about Virtual Machine", 2005;
[7] Soumyo Moitra and Suresh Konda, "A Simulation Model for Managing Survivability and Networked Information System", CMU/SEI-200-TR-20, Technical Report, 2000

Proceedings of the 13th International Conference on Quality and Dependability
Neptun, Romania, September 5th-7th, 2012
ISSN 1842-3566
Pages 200-206
[8] Nancy R. Mead, "Requirements Engineering for Survivable Systems", Tehnical Note CMU/SEI-2003-TN-013, 2003;
[9] Bernaschi, M., Grabrielli, E. and Mancini, L., "A Security- Enhanced Operating System", ACM Transactions on Information and System Security, Vol 5, 2001;
[10] Chen P. and Noble B., "When Virtual Is Better Than Real", Proceedings of the 2001 Workshop on Hot Topics in Operating Systems (HotOS);
[11] Howard Lipson, "Evolutionary Systems Design: Recognizing Changes in Security and Survivability Risks", CMU/SEI- 2006-TN-027, Technical Report, 2006.