

Asigurarea survivabilității sistemelor informatice complexe

**Costel CIUCHI, Laura IANCU, Gabriel PETRICĂ, Ioan
BACIVAROV, Angelica BACIVAROV**

EUROQUALROM Laboratory, ETTI, University POLITEHNICA of Bucharest, Romania
ciuchic@yahoo.com

Abstract

Defining essential capacities and fundamental quality attributes for systems are necessary to ensure optimum performance and to support strategies and objectives of an organization. Understanding the evolution of the quality characteristics and functionalities of the system in the presence of a fault can result from analyzing survivability – survival capacity of the system. Survivability can be defined as the set of technical and procedural measures taken to minimize the impact effect of an incident. Survivability has as fundamental purpose identifying the real costs of backup resources needed for restoration mechanisms to be added to a system to maintain services at a high level of performance. Survivability study of information systems, especially for Web applications, is a less explored domain in the literature. This article describes the SNA (Survivable Network Analysis) method in the context of Web applications developed on a 3-tier architecture through systematic evaluation of the proposed survival properties.

Keywords: survivability, security, strategy, SNA, decision, infrastructure.

References:

- [1] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff and N. R. Mead, „An Approach to Survivable Systems“, Technical Report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 1999.
- [2] R. J. Ellison, D. A. Fisher, R., C. Linger, H. F. Lipson, T. A. Longstaff and N. R. Mead, „Survivability: Protecting Your Critical Systems“, CERT Coordination Center Software Engineering Institute, IEEE Internet Computing, pp. 55-63, 1999.
- [3] Y. Liu and K. S. Trivedi, „A general framework for network survivability quantification“, 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems together with 3rd Polish-German Teletraffic Symposium (MMB & PGTS 2004), VDE Verlag, 2004, pp. 369-378.
- [4] R. J. Ellison, R. C. Linger, H. F. Lipson, N. R. Mead and A. Moore, „Foundations for Survivable Systems Engineering“, Technical Report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 2001.
- [5] SURVIAC – DoD Survivability / Vulnerability Information Analysis Center, www.bahdayton.com/surviac.
- [6] COM (2009) 149., COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR privind protecția infrastructurilor critice de informație „Protejarea Europei de atacuri cibernetice și

perturbații de amploare: ameliorarea gradului de pregătire, a securității și a rezilienței“, Bruxelles, 30.3.2009.

[7] Rezoluția Consiliului din 18 decembrie 2009 privind o abordare europeană a securității rețelilor și a informațiilor bazată pe colaborare (2009/C 321/01).

[8] COM (2011) 163, COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR privind protecția infrastructurilor critice de informație „Realizări și etape următoare: către un context global de securitate cibernetică“, Bruxelles, 31.3.2011.

[9] R. J. Ellison et al., „Survivable Network Systems: An Emerging Discipline“, Tech. Report CMU/SEI-97-TR-013, Pittsburgh, Penn., Software Engineering Institute, Carnegie Mellon University, Nov. 1997 (revised May 1999).

[10] Bacivarov, I., and Mihai, I.C., „The Survivability Analysis of the Informational Systems“, Proceedings of the 11th International Conference of Quality and Reliability – CFF2008, Sinaia, 24-26 September, 2008, pp. 151-158, ISSN: 1842-3566.

[11] I. C. Mihai, I. Bacivarov, „Survivability Analysis Based on Attack Models“, Proceedings of the XIIIth International Conference of Quality and Reliability – CFF2012, Neptun, 5-7 septembrie, 2012, pp. 200-206, ISSN: 1842-3566.

[12] A. Avizienis, J.-C. Laprie and B. Randell, „Fundamental concepts of computer system dependability“, IARP/IEEE Workshops on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments, Seoul, Korea, May 2001.

[13] Y. Liu and K. S. Trivedi, „Survivability Quantification: The Analytical Modeling Approach“, Int. Journal of Performability Engineering 2 No. 1 (2006): 29-44.

[14] C. Warren Axelrod, „The Dynamics of Privacy Risk“, Information Systems Control Journal, Vol. 3, 2004.

[15] [http://msdn.microsoft.com/en-us/library/windows/desktop/ms685068\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms685068(v=vs.85).aspx).S52

[16] Gary P. Schneider, „Electronic Commerce“, Third Annual Edition, Thomson Learning, 2002.

[17] <http://msdn.microsoft.com/en-us/library/ee658117.aspx>.

[18] R. Kazman, M. Klein, M. Barbacci, T. Longstaff, H. Lipson and S., J. Carriere, „The Architecture Tradeoff Analysis Method“, Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, IEEE Computer Society, 1998.

[19] Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff, John McHugh, „Survivable Network Analysis Method“, CMU/SEI-2000-TR-013, ESC-TR-2000-013, September 2000.

[20] R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, „A Case Study in Survivable Network System Analysis“, Technical Report CMU/SEI-98-TR-014 ESC-TR-98-014, September 1998.