

A Risk-Management Approach to the Design of Survivable COTS-Based Systems

Howard F. Lipson	Nancy R. Mead	Andrew P. Moore
hfl@cert.org	nrm@sei.cmu.edu	apm@cert.org
412-268-7237	412-268-5756	412-268-5465

CERT[®] Coordination Center
Software Engineering Institute
Pittsburgh, PA 15213 USA

© 2001 by Carnegie Mellon University

The indiscriminate use of COTS components is a primary impediment to the design of survivable systems. Lower upfront costs, and a belief that the cost savings extend throughout the system's lifecycle, are primary motivators in the shift from custom-designed to COTS-based systems. The disadvantages associated with COTS-based design include the absence of source code and the lack of access to the other artifacts of the software engineering process used to design the COTS components. These artifacts include architectural representations, comprehensive test results, results of (or even indications of the existence of) design reviews and code walkthroughs, and descriptions of (and the design rationale for) all explicit tradeoffs among the various attributes of software quality, such as performance, security, reliability, modifiability, usability, and cost. Moreover, the economic realities of mass-produced software bias these design tradeoffs in favor of lower costs and increased market share for the vendor, whereas survivability is largely dependent upon those software quality attributes (such as security and reliability) that support the mission of the acquiring organization.

Building survivable systems using COTS components is a daunting task because the artifacts of the software engineering process used to create the components are the primary sources from which assurance evidence for a composite system is derived. The lack of access to these artifacts is a major obstacle to the design of survivable systems using COTS components [Mead_01]. One way to partially compensate is to use vendor risk assessments as a tool to help you build, maintain, and evolve survivable systems. Such an assessment can be used as a new source of assurance evidence of a system's survivability.

Whether you've built your system using COTS components from many vendors, or a single vendor has provided you with an integrated solution, many of the risks associated with system management and operation are not in your direct control [Basili_01, Brownsword_00, Hissam_98, Lindqvist_98, Longstaff_01]. Each vendor that plays a role in the design, development, acquisition, integration, deployment, maintenance, operation, or evolution of part (or all) of your system affects the risks you face in your attempt to survive cyber-attacks,

[®] "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

accidents, and subsystem failures. We propose continual vendor-based risk evaluations as a critical part of the system lifecycle for mission-critical systems that use COTS components.

Our proposed vendor risk assessments [Lipson_01] are based on a *V-RATE* (vendor risk assessment and threat evaluation) taxonomy described below. Two broad categories are at the highest level of our taxonomy: (a) vendor-inherent risk elements and (b) vendor risk elements associated with your own risk management skills. The output of an assessment based on the V-RATE taxonomy is a vendor risk profile for the system being evaluated. We envision a large and growing collection of vendor risk profiles tied to real-world performance histories, providing empirical data against which a newly generated risk profile can be compared. A vendor risk profile can be used to assess the risk associated with the use of a product in a particular threat environment, and to identify areas for additional risk-mitigation activities. Because a single numerical rating would not provide sufficient guidance for these risk-mitigation activities, the vendor risk profile helps you to identify your risks in each of the V-RATE taxonomy areas, and allows you to consider your risk tolerance with respect to each element of the taxonomy.

Elements of the V-RATE taxonomy include:

1 Vendor's Inherent Risk Elements

1.1 Visibility of Product Attributes

- 1.1.1 Openness – Degree of visibility into design and engineering processes
- 1.1.2 Independent testing organizations

1.2 Technical Competence

- 1.2.1 Survivability capability maturity
- 1.2.2 Existence of vendor ratings/certifications
- 1.2.3 Evidence of adherence to applicable industry standards and government regulations.
- 1.2.4 Demonstrated diversity and redundancy in a vendor's products and services.
- 1.2.5 Existence of a vendor team that deals effectively with security/survivability issues

1.3 Performance History

1.4 Compliance

- 1.4.1 Willingness to customize
- 1.4.2 Responsiveness to feature requests
- 1.4.3 Responsiveness to security/survivability issues

1.5 Trustworthiness

- 1.5.1 Track record / Word-of-mouth
- 1.5.2 Evidence of skill at evaluating trustworthiness of personnel

1.6 Business Management Competence

- 1.6.1 Economic viability
- 1.6.2 Vendor's risk management skills in dealing with subcontractors

1.7 Controlled Evolution

- 1.7.1 Clearly specified (or discernable) evolutionary path
- 1.7.2 Product integration stability
- 1.7.3 Product evolution supports continual survivability improvement

2 Vendor Risk Elements Associated with Your Risk Management Skills in Dealing with Vendors

2.1 Technical Risk-Mitigating Factors

- 2.1.1 Your skill at product attribute evaluation
- 2.1.2 Your skill at evaluating vendor technical competence
- 2.1.3 Awareness of existing vendor ratings and certifications
- 2.1.4 Demonstrated diversity and redundancy in the integration of vendor products and services.
- 2.1.5 Use of architectural tools and techniques (e.g., wrappers) to limit risks associated with a vendor product.
- 2.1.6 Your association with expert security/survivability organizations, and the existence of a dedicated security/survivability group within your own organization.

2.2 Non-Technical Mitigation of Risk

- 2.2.1 Legal
- 2.2.2 Economic
- 2.2.3 Political and social

2.3 Independence / Interdependence (of your system's COTS components and services)

2.4 Your Exposure (i.e., extent of your reliance upon specific COTS products & vendors)

2.5 Your Mission Alignment (with vendor capabilities and vendor mission)

2.6 Your Negotiating Skill & Bargaining Power

The V-RATE method provides a framework for assessing risks associated with COTS products. Although there are many risks and much work to be done, there are specific ways that risk can be reduced. In the long term, we would like to see a full list of vendor risk reduction techniques. Each technique could be assigned a value that could be used in the V-RATE calculation to show reduction of overall risk associated with specific COTS products. Here is an example of a specific strategy that could be used to reduce risk in the Compliance area (1.4)

The vendor shows a willingness to respond to security and survivability concerns (1.4) by:

- Making security patches available quickly.
- Allowing client to 'turn off' unneeded features and thus reduce risk associated with unneeded features. In this way the client can select a 'core' set of needed services, not one size fits all.
- Building recovery mechanisms into the software. Examples of such mechanisms are automated back up of data and retention of state data.
- Building security (resistance) mechanisms into the software. Examples are encryption if needed, password protection, diversity.
- Putting specific practices in place to improve security, such as inspection, testing, use of strongly typed languages, and specific programming practices that reduce vulnerabilities.

In conclusion, to overcome the impediments imposed by COTS software on the design of survivable systems, we need to provide a means for both acquirers and vendors to understand the risks and work together to reduce them. As the V-RATE taxonomy indicates, our search for solutions must go beyond the purely technical realm to include economic, legal, political and social approaches within a risk-management framework.

Future work will investigate how to put V-RATE evaluations on a more scientific basis. A rigorous foundation for VRATE will require quantitative measures of a system's capability to survive malicious attacks, and ways to measure the contribution of a given COTS product (or set of COTS products) to promoting or impeding that capability. V-RATE may provide input into a CMM-like model that would help acquirers to more systematically assess a developer's maturity for producing COTS products for survivable systems. Finally, we need to apply V-RATE to real-world, mission-critical systems. Such case studies will help us to fine-tune and validate the method, and demonstrate its use within a realistic lifecycle process.

References

- [Basili_01]** V.R. Basili, B. Boehm, "COTS-Based Systems Top 10 List", *IEEE Software*, Volume 34, Number 5, May 2001, pp 91-93.
- [Brownsword_00]** L. Brownsword, P. Oberndorf, C. Sledge, "An Activity Framework for COTS-Based Systems," *Crosstalk: The Journal of Defense Software Engineering*, Vol. 13, No. 9, September 2000.
- [Hissam_98]** S.A. Hissam, D. Carney, D. Plakosh, *DoD Security Needs and COTS-Based Systems*, SEI Monographs on the use of Commercial Software in Government Systems, September 1998.
- [Lindqvist_98]** U. Lindqvist, E. Johnson, "A Map of Security Risks Associated with Using COTS," *IEEE Computer*, June 1998, pp. 60-66.
- [Lipson_01]** H. Lipson, N. Mead, A. Moore "Can We Ever Build Survivable Systems from COTS Components," Submitted for Publication, July 2001.
- [Longstaff_01]** T. A. Longstaff, C. A. Sledge, Y. Haimes, "COTS-Based Systems and the Risk to Information Assurance", Draft submitted for publication, April 2001.
- [Mead_01]** N.R. Mead, H.F. Lipson, C.A. Sledge, "Towards Survivable COTS-Based systems, *Cutter IT Journal*, Volume 14, No. 2, February 2001, pp. 4-11.