

Software Integrity Analysis Methodology

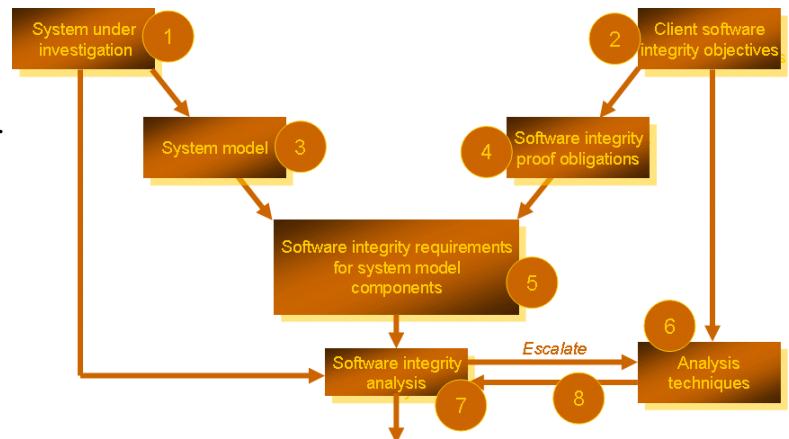
Gamma's software integrity analysis methodology is essentially unchanged since it was developed by Gamma's directors, Dr. David Brewer and Dr. Mike Nash, in the early 1980s.

We first determine what the system (1) is that the client wishes us to investigate and what the client wishes us to prove about it (2). We then model (3) the system and translate the client's requirements into axioms or other forms of proof obligations (4).

The idea is that if we can prove these then we will have demonstrated that the system meets the client's requirements. Some of these proof obligations exist to demonstrate that the model is a sufficiently good representation of the actual system under investigation for our results to be valid. Such proof obligations are usually confirmed by testing the system, but for systems that have been in operation for some time, other ways, such as analysis of live error reports may be more efficient.

However, for complex systems, for example, networked systems with many users, the system model is, by itself, insufficient and more detailed models, together with their associated proof obligations are re-

quired (5). Various analytical techniques are then used (6) to perform the analysis (7). Different techniques give results with different levels of confidence, but are often more expensive to perform. We therefore use the principle of escalation (8) whereby we only use a



Correct operation of the system under investigation with respect to the software integrity policy confirmed or deviations determined. The level of confidence in the answers is dependent on the analysis techniques used in the investigation.

superior technique on those areas of the system where greater confidence in the results is required by the client.

The results are usually expressed in the form of a report which records the objectives of the assignment, the manner in which it was conducted and the results that we obtained.

An example of the use of this methodology that is in the public domain is its application to an electronic funds transfer system for a bank. Please see www.gammassl.co.uk/topics/hot3.html.

For further information, please contact Dr. David Brewer

ISO/IEC 27001 and ISO 9000 certified for the provision of information security consultancy



Gamma Secure Systems Limited

Diamond House
149 Frimley Road
Camberley, Surrey
GU15 2PS, United Kingdom

Phone: +44 1276 702500

Fax: +44 1276 692903

www.gammassl.co.uk

E-mail: dbrewer@gammassl.co.uk