

Assurance Cases for Security: The Metrics Challenge

Robin Bloomfield¹, Marcelo Masera², Ann Miller³, O. Sami Saydjari⁴, Charles B. Weinstock⁵

¹Center for Software Reliability, ²Joint Research Center of the European Commission,

³University of Missouri at Rolla, ⁴Cyber Defense Agency, ⁵Software Engineering Institute
reb@csr.city.ac.uk, marcelo.masera@jrc.it, milleran@umr.edu,
ssaydjari@CyberDefenseAgency.com, weinstock@sei.cmu.edu

Abstract

For critical systems it is important to know whether the system is trustworthy and to be able to communicate, review and debate the level of trust achieved. In the safety domain, explicit Safety Cases are increasingly required by law, regulations and standards. Yet the need to understand risks is not just a safety issue and the type of argumentation used for safety cases is not specific to safety alone.

Prior workshops, beginning with one held at DSN 2004, have identified a number of technical, policy and research challenges. The focus of this workshop is on one of these challenges: metrics for assurance cases for security.

1. Introduction

For critical systems it is important to know whether the system is trustworthy and to be able to communicate, review and debate the level of trust achieved. In the safety domain, explicit Safety Cases are increasingly required by law, regulations and standards. It has become common for the case to be made using a goal-based approach, where claims (or goals) are made about the system and arguments and evidence are presented to support those claims.

The need to understand risks is not just a safety issue: more and more organizations need to know their risks and to be able to communicate and address them to multiple stakeholders. The type of argumentation used for safety cases is not specific to safety alone, but it can be used to justify the adequacy of systems with respect to other attributes of interest including security, reliability, etc.

An international community has begun to form around this issue of generalized assurance cases and the challenge of moving from the rhetoric to the reality of being able to implement convincing and valid cases. In a recent article in IEEE Security and Privacy [1] we

outline what we have been doing so far in the security area, what we hope to achieve and where we go next.

Prior workshops, beginning with one held at DSN 2004, have identified a number of technical, policy and research challenges. This workshop will focus on one of these challenges: metrics for assurance cases for security.

2. The Importance of Metrics

Metrics can be essential for supporting decisions regarding the resources provided to develop the assurance case, and the efficacy of the resulting case. However, there is no commonly accepted approach to this topic. The purpose of this workshop is to identify the state of the practice in metrics for assurance cases in the specific context of security, identify promising ways forward and research directions.

We expect that the workshop will produce the following outputs:

1. Identification of the candidate metrics for assurance cases for security and the characteristics which those metrics must possess.
2. A listing of the major classes of evidence for assurance cases for security and a mapping of classes of evidence to metrics.
3. Candidate methods for combining the various classes of evidence toward the desired system security properties.

3. Questions to be Answered

In the context of security the workshop will answer questions such as:

1. What makes an argument compelling?
2. Are there standard patterns for arguments?
3. What arguments should be compelling? What arguments do people actually find compelling?
4. How do additional arguments or evidence serve to increase the compelling nature of a case?

5. If there are accepted notions of what makes a case compelling, to what extent do we know that these accepted notions are correct or incorrect?
6. Is there a measure of compellingness that could be used to compare alternative argumentation structures?
7. How can assurance cases be composed? If they are composed, is it also possible to compose the metrics associated with the individual cases?
8. How can arguments with different compelling force be compounded for supporting the case claims?
9. What new types of evidence are needed to create arguments which are more sound and how will we measure that they are more sound?
10. By what metrics do we assess the effectiveness of evidence?
11. What is the cost/benefit justification for developing an assurance case?
12. Are there different levels of effort depending on the motivation? Can these levels be quantified?
13. Can it be shown that a well-defined and executed assurance case process will cost less than current assurance processes?

14. Given two cases, one that costs more and, by some metric, is more compelling than the other, how does one make the trade?

4. Format and Expected Output

The one day workshop will be held on Wednesday, June 27, 2007. An invited talk will be followed by brief presentations by those who have previously submitted position papers. The “toy” example developed at the June 2005 workshop referenced in [1] will be presented and used to motivate and focus the ensuing discussions. A breakout session will be formed if appropriate and at the end of the day a consolidated report and conclusions will be presented.

5. References

- [1] Robin E. Bloomfield, Sofia Guerra, Ann Miller, Marcelo Masera, and Charles B. Weinstock, "International Working Group on Assurance Cases (for Security)," *IEEE Security & Privacy*, vol. 4, no. 3, May/June 2006, pp. 66-68.