Representation of Knowledge in the Dependability Domain

Algirdas Avižienis
Vytautas Magnus University
Kaunas, Lithuania and
University of California
Los Angeles, USA

A Question about Terms

- Dependability and Security
- Trustworthiness
- Survivability
- High Confidence
- Information Assurance
- Robustness
- Resilience
- Fault Tolerance
- Self – Healing

How do they differ?

Looking for the Difference

- Property X protects the system from delivering “bad” service in a given environment, where “bad” means

  that the service does not satisfy the system function.
- We describe X by three answers

Description of X

- What *threats* are expected that can cause “bad” service ?
- Which defense techniques does X employ ?
- How is the success of X measured ?

The answers for all terms X are very similar

Concept	Dependability	High Confidence	Survivability	Trustworthiness
Goal	1) ability to deliver service that can justifiably be trusted 2) ability of a system to avoid service failures that are unacceptably frequent or severe	consequences of the system behavior are well understood and predictable	capability of a system to fulfill its mission in a timely manner	assurance that a system will perform as expected
Threats present	1) development faults (e.g., software flaws, hardware errata, malicious logic) 2) physical faults (e.g., production defects, physical deterioration) 3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)	• internal and external threats • naturally occurring hazards and malicious attacks from a sophisticated and well-funded adversary	1) attacks (e.g., intrusions, probes, denials of service) 2) failures (internally generated events due to, e.g., software design errors, hardware degradation, human errors, corrupted data) 3) accidents (externally generated events such as natural disasters)	1) hostile attacks (from hackers or insiders) 2) environmental disruptions (accidental disruptions, either man-made or natural) 3) human and operator errors (e.g., software flaws, mistakes by human operators)

The Representation Problem

Multiple near-synonymous terms exist

Disadvantages that impair progress:

- Continuing re-invention
- Plagiarism
- Confusion among potential users
- Difficulties for referees and evaluators

The Need: a single thesaurus and ontology of dependable and secure computing

Sad Conclusion: a committee of volunteers or bureaucrats cannot do it!

A Potential Solution

Apply computer tools for human language processing

- Extract ***term candidates*** from a set of texts
- Build a ***thesaurus***: list of important terms and related terms for each entry of the list
- Build an ***ontology***: data model that represents the thesaurus
- Perform ***automatic classification*** of texts using automatic indexation and clustering tools

The Problem is Common for All of Computer Science & Engineering

- The only taxonomy of Computer S&E is the ACM CSS (Computing Classification System) devised in 1988, revised in 1998
- Dependability and security are inadequately treated in the ACM CSS
- The Challenge: a major revision of the ACM CSS is being initiated, therefore our thesaurus and ontology must be ready

A Search for Consensus

IEEE Computer Society: TC on Fault-Tolerant Computing (1970)

IFIP: WG 10.4 “Dependable Computing and Fault Tolerance” (1980)

1982: Special session at FTCS-12: several concept papers

1985: Synthesis: J.C.Laprie paper at FTCS-15

1992: Six-language book “Dependability: Basic Concepts and Terminology”

2004: “Basic Concepts and Taxonomy of Dependable and Secure Computing” in IEEE Trans. on Dependable and Secure Computing, Vol.1, no.1

An “Info-Skeptic” view

- Physical sciences study nature: given phenomena
- Computer S&E study information: human-made concepts
- The concepts should compete, and the fittest will survive!
- If a good concept disappears, it will reappear again,

  with some luck… in my research