Software Assurance Principles

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Principles of software assurance

A set of principles to guide learners in understanding the WHY as well as the WHAT and HOW of software assurance

- Easy to learn
- Easy to remember
- First step for learning software assurance

Definitions

Software assurance (Software Assurance Curriculum Project)

> Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

Principle (Free Merriam-Webster Dictionary)

1 *a* **:** a comprehensive and fundamental law, doctrine, or assumption *b (1)* **:** a rule or code of conduct *(2)* **:** habitual devotion to right principles <a man of *principle*> *c* **:** the laws or facts of nature underlying the working of an artificial device

2**:** a primary source **:** origin

3 *a* **:** an underlying faculty or endowment <such *principles* of human nature as greed and curiosity> *b* **:** an ingredient (as a chemical) that exhibits or imparts a characteristic quality — **in principle:** with respect to fundamentals <prepared to accept the proposition *in principle*>

Basis: References

- Saltzer and Schroeder's categories: environmental considerations and technical underpinnings
- Software Assurance Reference Curriculum Core Body of Knowledge (Software Assurance Curriculum project)
- Software Assurance Drivers (Alberts, Christopher; Allen, Julia: & Stoddard, Robert. Integrated Measurement and Analysis Framework for Software Security (CMU/SEI-2010-TN-025). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/reports/10tn025.pdf)
- Seven dimensions of computation, communication, coordination, recollection, automation, evaluation, and design (http://greatprinciples.org)

Basis: Core Team

SEI Participants:

- Carol Woody, (project lead)
- Nancy Mead
- Robert Ellison
- Christopher Alberts

Reviewers:

- Dan Shoemaker
- Oxford Computing Center
- London South Bank University

Principle 1: Risk

Perception of risk drives assurance decisions

- Assurance implementation choices (policies, practices, tools, restrictions) are based on the perception of threat and the impact should that threat be realized
- Perceptions are built based on successful attacks – the current state of assurance is largely reactive – more successful organizations react and recover faster, learn from the reactive responses or others, and are more vigilant in anticipating and detecting attacks
- Misperceptions are failure to recognize threats and impacts – “how could it happen to us?”
- Risk decisions must be shared among all stakeholders and technology participants to ensure a consistent and effective implementation

Principle 2: Interactions

Highly connected systems (e.g. Internet) require alignment of risk across all stakeholders otherwise critical threats will be unaddressed (missed, ignored) at different points in the interactions

- There are costs to addressing assurance which must be balanced against the impact of the risk
- Risk must also be balanced with other opportunities (performance, reliability, usability, etc.)
- Interactions occur at many technology levels (network, security appliances, architecture, applications, data storage, etc.) and are supported by a wide range of roles – effective assurance requires consist risk recognition and response at all levels

Principle 3: Trusted Dependencies

Your assurance depends on other people’s assurance decisions and the level of trust you place on these dependencies (system of system problem based on interactions)

- Each dependency represents a risk
- Dependency decisions should be based on a realistic assessment of the threats, impacts, and opportunities represented by an interaction
- Dependencies are not static and trust relationships should be reviewed to identify changes that warrant reconsideration
- Using many standardized pieces to build technology applications and infrastructure increases the dependency on other’s assurance decisions

Principle 4: Attacker

There exists a broad community of attackers with growing technology capabilities able to compromise the confidentiality, integrity, and availability of any and all of your technology assets - there are no perfect protections and the attacker profile is constantly changing.

- The attacker uses technology, processes, standards, and practices to craft a compromise (socio-technical responses).
- Attacks are crafted to take advantage of the ways we normally use technology or designed to contrive exceptional situations where defenses are circumvented

Principle 5: Everyone is Involved

Assurance requires effective coordination among all technology participants and their governing bodies

- Protection must be applied broadly across the people, processes, and technology because the attacker will take advantage of all possible entry points
- Authority and responsibility must be clearly established at an appropriate level in the organization to ensure effective participation

Principle 6: Assurance Must be Dynamic

An adaptive response is required for assurance (justified confidence that software functions as intended) because the threat is always changing. Assurance implementation must represent a balance among governance, construction, and operation and is highly sensitive to changes in each of these areas

- Engineering challenge: Assurance cannot be added later; you must build to the level of acceptable assurance that you need
- No one has resources to redesign systems every time the threat changes
- Assurance cannot be readily adjusted upward after the fact

Principle 7: Assurance Must be Measurable

A means to measure and audit overall assurance must be built in. If you can't measure it you can't manage it

- All elements of the socio-technical environment must tie together (practices, processes, procedures, etc.)
  - Measuring individual elements may be useful but not sufficient evidence for overall assurance
  - Each participant will address only the assurance for which they are held accountable
- Effective measurement is well supported by sound engineering and organizational principles - well formed and consistently applied processes are critical to ensure an appropriate measurable response

Themes

- **Communication** – successfully addressing the principles will require effective communication among stakeholders and technology participants;
- **Culture of sharing** – when participants have a culture of sharing there is a greater likelihood that information important to assurance will be effectively communicated; when this sharing includes formal documentation there is a greater likelihood that the information will persist
- **Traditional boundaries may be barriers** – organizational boundaries, system boundaries, contract boundaries, classification boundaries may inhibit critical communication of risks, threats, impacts, measures, etc. critical to software assurance
- **Complexity** increases the challenges for assurance and must be managed through the use of effective software engineering

Contact Information

Carol Woody

(412) 268-9137

cwoody@cert.org

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/