Overview

The Center for Software Engineering (CSE) at the University of Southern California (USC) is extending the widely-used Constructive Cost Model version 2 (COCOMO II) [Boehm, Abts, et al. 2000] to account for developing secure software. CSE is also developing a model for estimating the cost to acquire secure systems, and is evaluating the effect of security goals on other models in the COCOMO family. We will present the work to date.

Background

Engineering security in software-intensive systems is now a high-priority objective for the U.S. Federal Aviation Administration (FAA), which is supporting this research, for the U.S. Government generally, and for many industries. Prudent management is concerned about the life-cycle cost of security.

While it is widely held that engineering security will substantially raise software-project cost, different models vary in estimating the added cost. For example, [Bisignani and Reed 1988] estimates that engineering highly-secure software will increase costs by a factor of 8; the 1990’s Softcost-R model estimates a factor of 3.43 [Reifer 2002].

Both of these models are based on the 1985 Department of Defense Standard 5200.28-STD, “Trusted Computer System Evaluation Criteria” (called the “Orange Book”) [National Computer Security Center 1985]. However, the Orange Book, and cost models based on it, are obsolete. The ISO Standard Common Criteria for Information Technology Security Evaluation (CC) [ISO JTC 1/SC 27 1999a, b, c] has replaced the Orange Book.

COCOMO II provides an excellent base for developing and calibrating a software-cost driver for security. CSE over the past three years has been extending COCOMO II to produce COSECMO, a model for costing secure software-intensive systems.

Presentation

We will present CSE’s model COSECMO, based on the following analysis of behavior.

- Analyzed industry practices with respect to security (including standards like the Common Criteria).
- Analyzed the 149 Security Targets registered on the National Information Assurance Partnership (NIAP) Website (a collaboration of National Institute of Standards & Technology (NIST), and National Security Agency (NSA)).
- Conducted preliminary surveys of experts in software development and security.
COSECIMO introduces a new cost driver, and defines guides for setting other COCOMO drivers when costing the development of a secure system.

CSE has also developed a preliminary model for estimating the cost for development or acquisition of a secure system, for early use e.g. at Investment or Mission Analysis in FAA terms, based on typical work–breakdown structures to which we added security activities. Project life–cycle cost is estimated by identifying major cost sources, estimating the cost for each (e.g. by unit cost), and summing the result.

CSE has developed prototype tools that can be used to test and validate the two models.

Author Biographies

Ed Colbert, Senior Research Associate at CSE, is currently leading research on estimating the costing of developing secure systems. He is a contributor to CSE’s Model–Based (System) Architecting and Software Engineering (MBASE), and is consulting on the definition of an Architecture Design Language for real–time, safety–critical systems that is the standard of the Society of Automotive Engineers (SAE). The Colbert Object–Oriented Software Development method (“OOSD”), used by twenty commercial and government organizations, was chosen for the NASA Langley Research Center Software Engineering Process manual. Ed is a Senior Member of the Institute of Electrical & Electronics Engineers (IEEE) and a member of the International Council of System Engineers (INCOSE). He is pursuing his Ph.D. in Computer Science at CSE. (M.S. Computer & Communication Sciences 1981, B.S. Chemistry and Biology 1979, U. Michigan.)

Dan Wu, Ph.D. student at CSE, is researching process improvement and cost estimation for developing secure systems, including security extension on COCOMO. (B.S. Computer Science 2000, Southeast University, China.)

Yue Chen, Ph.D. student at CSE, is researching secure software engineering, software economics and processes. (M.E. Electrical Engineering 2001, B.E. 1997, University of Science & Technology, China.)

Barry Boehm, TRW Professor of Software Engineering and CSE Director, has current research interests in value–based software engineering, including MBASE. Among his contributions to the field are COCOMO, the Spiral Model of the software process, the Theory W (win-win) approach to software management and requirements determination, and the foundations for the areas of software risk management and software quality factor analysis. He was previously Director of the DARPA Information Science & Technology Office and the DDR&E Software & Computer Technology Office (U.S. Dept. of Defense); Chief Scientist of the TRW Defense Systems Group; and Head of the RAND Corporation Information Sciences Department. (Ph.D. Mathematics 1964, M.S. 1961, UCLA; A.B. Harvard 1957; Sc.D. (hon.) Computer Science 2000, U. Mass.)