Cost Estimation for Secure Software & Systems 2006 Project Update

Ed Colbert	Dan Wu	Yue Chen	Dr. Barry Boehm
ecolbert@usc.edu	danwu@usc.edu	yuec@cse.usc.edu	boehm@usc.edu
(213) 821-1240	(213) 740-9731	(213) 740-9731	(213) 740-8163

Center for Software Engineering
University of Southern California
941 W. 37th Pl.
Los Angeles, CA 90089-0781

Project Objectives

The Center for Software Engineering (CSE) at the University of Southern California (USC) is extending the *Constructive Cost Model* version 2 (*COCOMO II*) [Boehm, Abts, et al. 2000], which is widely used to estimate the cost of and schedule for developing software–intensive systems, to incorporate the effects of 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 (e.g. COCOTS, which is used to estimate the cost of systems that are mostly developed *Commercial–off–the–Shelf* (*COTS*) software).

Background

Engineering security in software–intensive system 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. Legislation and guidance from the U.S. Congressional Office of Management and Budget (OMB) requires each U.S. agency to plan and budget for security throughout the life–cycle of a system. Prudent management in industry is also concerned about the life–cycle cost of security.

While it is widely held that engineering security will substantially raise software–project cost, there has been wide variation in the amount of added cost estimated by different models. 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, security engineering has changed since the Orange Book.. Software technology has come to include features like distributed and mobile components, and commercial off–the–shelf ("COTS") components, and the Internet. Developers must now consider high–risk threats not only from foreign governments, or from amateurs, but also from well–funded and possibly well–trained terrorist groups. The Orange Book, and cost models based on it, is 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.

The USC's *Constructive Cost Model* version 2 (*COCOMO II*) [Boehm, Abts, et al. 2000] provides an excellent base for developing and calibrating a software–cost driver for security. Its advantages include:

- A completely open description of its cost–driver parameters and algorithms;
- Documented statistical calibration of its parameters to a body of carefully collected data points from approximately 200 projects;
- A proven methodology for extending the model to refine or add parameters;
- Compatibility with the current USC CSE analysis to provide a security extension to the COCOTS model.

Accomplishments to Date

Over the last three years, USC CSE has developed a model for costing secure software–intensive systems (*COSECMO*) based on USC CSE's methodology for extending COCOMO II. COSECMO is based on the following behavior–analysis activities.

- We analyzed industry practices with respect to security (including standards like the *Common Criteria*).
- We analyzed the 149 Security Targets registered on the National Information Assurance Partnership (NIAP) Website (which is a collaboration between the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA)).
- We conducted preliminary surveys of experts in software development and in security.

COSECMO introduces a new cost driver, and defines guides for setting other COCOMO drivers when costing the development of a secure system.

USC CSE has also developed a preliminary model for estimating the cost for development or acquisition of a secure system that can be used early in the project life–cycle, e.g. *Investment* or *Mission Analysis* in FAA terms. This *Early Cost Estimation* model is based on typical work–breakdown structures to which we added security activities. Project life–cycle cost is estimated by identifying major cost sources for activities; estimating the cost for each source via one of four mechanisms (e.g. unit cost); and summing the result.

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

Future Plans

USC CSE will continue to refine COSECMO and the Early Cost Estimation model by surveying a broader audience of software engineering and security experts, and by collecting and analyzing project data. USC CSE is also looking at expanding the two models to include safety–critical systems, the development of which shares many of the same concerns.

