

Security Extensions to COCOMO II Workshop Report

Ed Colbert &
Murali Gangadharan (CISSP)
{ecolbert,murali}@usc.edu



Center
For
**Software
Engineering**

Outline

Highlights

Progress

Issues

To Do

Highlights

❑ Multi-faceted Problem

– At least 2 drivers

- Size

$$\text{Size}_{\text{total}} = \text{Size}_{\text{base}} + \text{Size}_{\text{security}}$$

- Multiplier

– If > 2 drivers, probably unacceptable

❑ Scale factors

– Good start (“Right On”)

Highlights (cont.)

- ❑ Common Criteria emphasize secure devices, not systems
 - Goal: protecting box
 - Trend:
 - Can't prevent intrusion
 - Code has to reduce loss when attacked

- ❑ Proposed Model is based on Common Criteria
 - Ratings not tied to Evaluated Assurance Level (EAL)
 - Used EAL activities
 - Greater flexibility w/r to commercial strategies

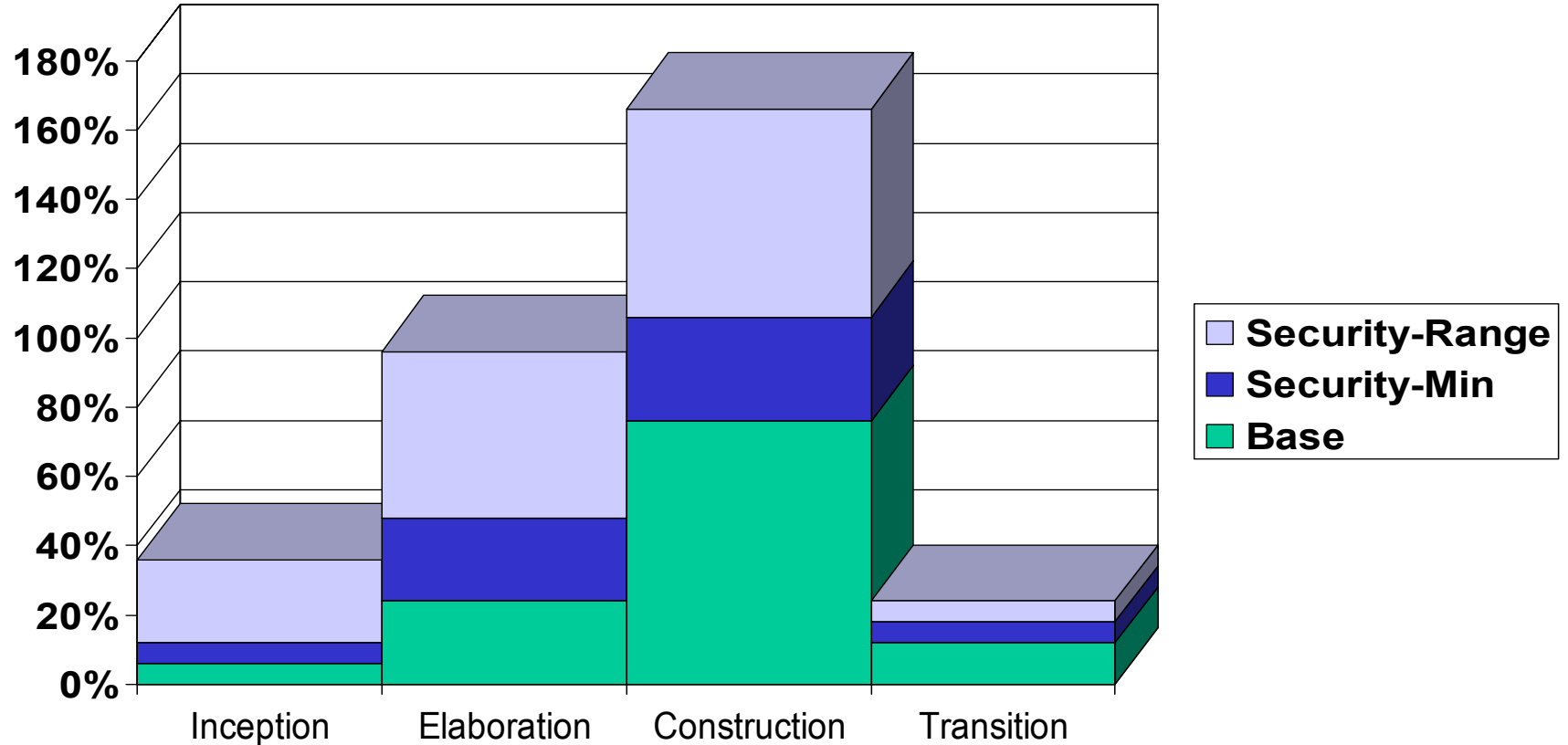
Progress

- ❑ Narrowed the analysis
 - Post-Architecture
 - Development life-cycle
 - See next slide

- ❑ Improved understanding of size based on Security Strategy
 - Need early estimate

- ❑ Name of the Model
 - We're not going to tell you (**Top Secret**)

Security Effect on Development Life–Cycle



❑ General Concepts

– Security %'s are just for show

Issues

- ❑ Keep model reasonable so can be used
- ❑ Is cost/LOC same for security code as ordinary code?
 - e.g. Cryptography
- ❑ Need to attract participation of
 - Commercial
 - Security Community
- ❑ Need to define model so acceptable to commercial developers

Issues (cont.)

- ❑ Behavior activities:
 - At what level can we measure?
 - Can we define SECU driver by multiplying activity ratings?
 - Lots of Delphi's?

- ❑ Relation to other "-ilities"
 - Reliability
 - Dependability
 - Safety

- ❑ What data do we want?
 - Can we get data from secure projects?

To Do

- Refine Behavior
 - Commercial
 - Security Community

- Develop Delphi

- Collect & Analyze Data

- Write Ph.D. thesis