

Security Extensions to COCOMO II

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



Center
For
Software
Engineering

Goal Of Presentation

- ❑ Review proposed extensions to COCOMO for development of Secure Systems
 - 1-3 Drivers
 - Determination of ratings
 - Relation to *Common Criteria's Assurance Levels*

- ❑ Kick-off
 - Delphi Process
 - Behavior Analysis

Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ How to Extend COCOMO
- ❑ Draft Security Driver & Its Factors
- ❑ Analysis of Security Impact On Other Drivers
- ❑ Purpose of Workshop
- ❑ Summary

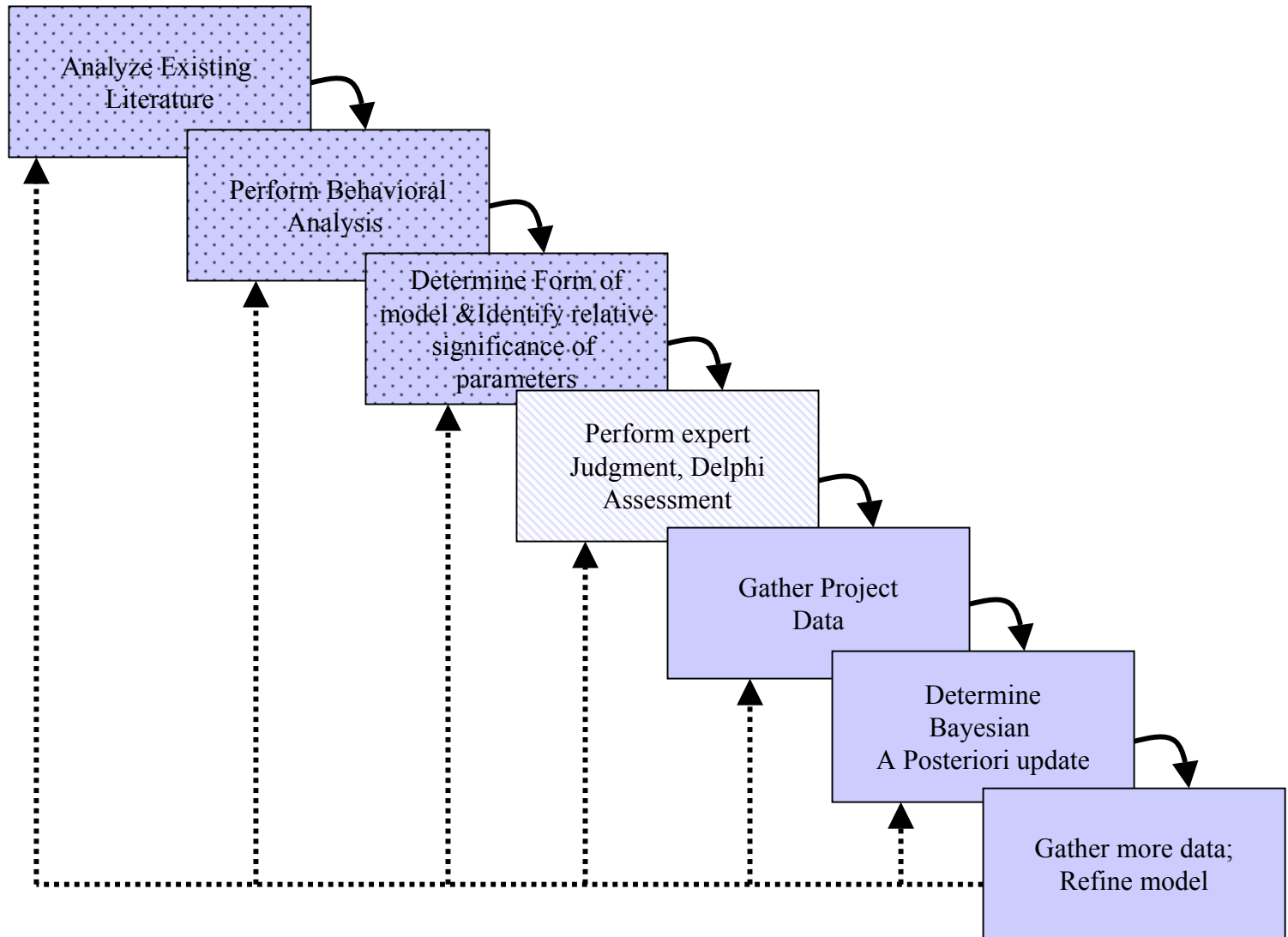
Why Extend COCOMO II for Security

- ❑ Military projects have considered security in developing software since the early 1980s
- ❑ Until recently commercial projects often gave it little weight
- ❑ Threat to business-critical systems & private information has grown
 - Security can no longer be ignored
- ❑ Few cost models (including COCOMO II) include security factors
 - Based 1980s military perspective (Orange Book)
 - Developing secure systems has changed dramatically

Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ **How to Extend COCOMO**
- ❑ Draft Security Driver & Its Factors
- ❑ Analysis of Security Impact On Other Drivers
- ❑ Purpose of Workshop
- ❑ Summary

COCOMO II Modeling Methodology



Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ **How to Extend COCOMO**
- ❑ **Draft Security Driver & Its Factors**
- ❑ Analysis of Security Impact On Other Drivers
- ❑ Purpose of Workshop
- ❑ Summary

Security Driver (SECU)

□ Rating Factors

- Physical Security
- Operational Security
- Development for Security

□ Ratings

- Ad hoc Defense (Low)
- Passive Defense (Nominal)
- Perimeter Defense (High)
- Layered Defense (Very High)
- Defense in Depth (Extremely High)

Conceptual Mapping of SECU Rating Levels to Common Criteria Assurance Levels

Driver Rating	Common Criteria Assurance Level
Extremely High (XH)	EAL-6
Very high (VH)	EAL-5
High (H)	EAL- 3&4
Nominal (N)	EAL-1,2
Low (L)	-

Security Driver Rating Factors

❑ Development for Security

- Effect of processes for development & validation of security-critical software

❑ Operational Security

- Effect of audit & monitoring mechanisms, tools, & facilities that
 - Permit identification of security events
 - Subsequent actions to identify key elements
 - Report pertinent information to appropriate individual, group, or process

❑ Physical Security

- Constraints due to protecting software development facility
 - From outside perimeter to inside office space
 - Includes all of information system resources

Development for Security

Rating Description: Low & Nominal

Low

- No security requirements
- No protection other than provided execution environment

Nominal

Requirements	<input type="checkbox"/> Informal security requirements formulated for system
Design	<input type="checkbox"/> Analysis of security functions using <ul style="list-style-type: none">– Informal functional & interface specification– Descriptive high-level design– Demonstration of corresponding pairs
Testing	<input type="checkbox"/> Developer tests implementation of requirements <ul style="list-style-type: none">– Black box testing
Life-cycle controls	<input type="checkbox"/> Simple Configuration Management (CM) with version numbers

Development for Security Rating Description: High

Nominal +

Requirements	<input type="checkbox"/> Fully defined external interfaces <input type="checkbox"/> Informal security policy modeling
Design	<input type="checkbox"/> Security enforcing high-level design <input type="checkbox"/> Informal low-level design description
Testing	<input type="checkbox"/> Independent testing of all functional requirements <input type="checkbox"/> Inspection of COTS source code if available
Life-cycle controls	<input type="checkbox"/> CM with unique referencing <input type="checkbox"/> Detailed delivery & installation procedures <input type="checkbox"/> Identification of security measures for life-cycle

Development for Security

Rating Description: Very High

High+

Requirements	<input type="checkbox"/> Semi-formal functional specifications <input type="checkbox"/> Formal security policy modeling
Design	<input type="checkbox"/> Semi-formal high-level design <input type="checkbox"/> Modular implementation <input type="checkbox"/> Wrapper & dynamic analysis for COTS & Open-source
Testing	<input type="checkbox"/> Evidence of coverage for all developer test results <input type="checkbox"/> Testing of high-level design <input type="checkbox"/> Independent vulnerability analysis <input type="checkbox"/> Independent validation of analysis
Life-cycle controls	<input type="checkbox"/> Partial automation of CM – with authorization control, problem tracking, & detection of modification <input type="checkbox"/> Developer-defined life-cycle model – with well-defined development tools

Development for Security

Rating Description: Extremely High

Very High +

Requirements	<input type="checkbox"/> Fully defined external interfaces <input type="checkbox"/> Informal security policy modeling
Design	<input type="checkbox"/> Semi-formal high level explanation <input type="checkbox"/> Structured implementation with reduction of complexity <input type="checkbox"/> Secure container for COTS and Open-source
Testing	<input type="checkbox"/> Analysis of coverage of tests <input type="checkbox"/> Ordered functional testing with tests of low-level design <input type="checkbox"/> Covert channel analysis
Life-cycle controls	<input type="checkbox"/> Compete automation of CM – with coverage for developer tools <input type="checkbox"/> Standardized life-cycle model – with compliance to implementation standards

Operational Security

Rating Description: Low & Nominal

Low

- No organization-wide security policies.
- Ad-hoc security practices.
- Optional firewall & virus protection

Nominal

Administration	<input type="checkbox"/> Security policies are well defined <ul style="list-style-type: none">– inc.<ul style="list-style-type: none">• Password and Virus Protection policy• Network access and system use policy <input type="checkbox"/> Proper guidance documentation for administrators & users
Protection	<input type="checkbox"/> Reasonable practices for <ul style="list-style-type: none">– Checksum verification– Software firewall(s)– Operating system logging
Authentication	<input type="checkbox"/> Simple password-based authentication schemes

Operational Security Rating Description: High

Nominal +

Administration	<input type="checkbox"/> Security policies are well defined <ul style="list-style-type: none">– inc.<ul style="list-style-type: none">• Incident Response policy• Data classification policy <input type="checkbox"/> Documentation & logging of all security incidence
Protection	<input type="checkbox"/> Reasonable practices for <ul style="list-style-type: none">– Hardware firewalls– Public Key Infrastructures– Passive system & network monitoring
Authentication	<input type="checkbox"/> Two factor authentication using passwords & soft-tokens

Operational Security

Rating Description: Very High

High +

Administration	<input type="checkbox"/> Security policies are well defined <ul style="list-style-type: none">– inc.<ul style="list-style-type: none">• Business continuity plans• Disaster recovery plans <input type="checkbox"/> Incident response teams handles security breaches
Protection	<input type="checkbox"/> Reasonable practices for <ul style="list-style-type: none">– Proxy servers– Private-key encryption– Active system monitoring with Intrusion Detection Systems
Authentication	<input type="checkbox"/> Digital certificates & signatures used for <ul style="list-style-type: none">– Authentication– Non-repudiation

Operational Security

Rating Description: Extremely High

Very High +

Administration	
Protection	<input type="checkbox"/> Reasonable practices for <ul style="list-style-type: none">– Active systems monitoring– Network monitoring– “Honey pots”
Authentication	<input type="checkbox"/> Multi-factor authentication with biometrics

Physical Security Rating Description

Nominal

- None

High

- All source materials are locked up when not in active use

Very High

- High +

- Audited security markings in code

Extremely High

- Very High+

- Multi-compartment developer communication constraints

Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ **How to Extend COCOMO**
- ❑ **Draft Security Driver & Its Factors**
- ❑ **Analysis of Security Impact On Other Drivers**
- ❑ Purpose of Workshop
- ❑ Summary

Existing COCOMO Drivers Affected By Security

- ❑ Proposed security cost driver (SECU) constrain existing COCOMO II cost drivers

RELY	Required software reliability
CPLX	Product complexity
DOCU	Documentation match to life-cycle needs
SITE	Multi-site development
TOOL	Use of software tools

- ❑ Security functions add to project's size
- ❑ Increases project risk

Security Effect On Reliability

- ❑ Requires increased reliability
 - Due to activities like
 - High-integrity design
 - Verification & validation

- ❑ Forces higher project value for RELY ratings

SECU Rating	RELY Rating Constraint
LO	-
NOM	\geq LO
HI	\geq NOM
VHI	\geq HI
XHI	\geq VHI

Security Effect on Complexity

- ❑ Increases project complexity
 - Due to activities like
 - Formal proofs of security
 - Security tradeoff analysis

- ❑ Forces higher project value for CPLX rating

SECU Rating	CPLX Rating Constraint
LO	-
NOM	\geq LO
HI	\geq NOM
VHI	\geq HI
XHI	\geq VHI

Security Effect on Documentation

- ❑ Increases life-cycle documentation
 - e.g.
 - Vulnerability & threat assessment documentation
 - User & Administrator guidance documentation

- ❑ Forces higher project value for DOCU rating

SECU Rating	DOCU Rating Constraint
LO	-
NOM	\geq NOM
HI	\geq NOM
VHI	\geq HI
XHI	\geq HI

Security Effect on Multi-site Development

- ❑ Additional effort required to secure communication
 - e.g. Virtual Private Networks
- ❑ Forces higher project value for SITE rating

SECU Rating	SITE Rating Constraint
LO	-
NOM	\geq LO
HI	\geq NOM
VHI	\geq HI
XHI	=VHI

Security Effect on Use of Software Tools

- ❑ Increases Software Tools required
 - e.g.
 - Static Code checkers
 - Attack modeling tools

- ❑ Forces higher project value for TOOL rating

SECU Rating	TOOL Rating Constraint
LO	-
NOM	\geq LO
HI	\geq NOM
VHI	\geq HI
XHI	=VHI

Security Effect on SIZE

❑ Development for Security

- Authentication functions
- Authorization functions
- Privacy & copyright protection functions
- Accountability & non-repudiation functions
- Integrity functions
- Detection & monitoring functions
- Availability functions

❑ Operational Security

- Incident response
- Activity logging
- Trend analysis

Security Effect on Risk

- ❑ Projects risk is increased when
 - Security driver rating is \geq high
 - Rating of following drivers are \leq low
 - ACAP : Analyst Capability
 - PCAP : Programmer Capability
 - APEX : Application Experience
 - PLEX : Platform Experience
 - LTEX : Language Experience

Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ **How to Extend COCOMO**
- ❑ **Draft Security Driver & Its Factors**
- ❑ **Analysis of Security Impact On Other Drivers**
- ❑ **Purpose of Workshop**
- ❑ **Summary**

Purpose of Workshop

- ❑ Identify impact of security for each life-cycle activity
 - Inception
 - Elaboration
 - Construction
 - Transition
 - Maintenance
- ❑ Define
 - Cost driver(s)
 - Based on proposal?
 - *Specific Scale &/or Multiplicity Factors*
 - Ratings
 - “Delphi” for rating impact
 - Effect on other COCOMO II drivers
- ❑ Identify anything missed

Outline

- ❑ **Why Extend COCOMO II for Security?**
- ❑ **How to Extend COCOMO**
- ❑ **Draft Security Driver & Its Factors**
- ❑ **Analysis of Security Impact On Other Drivers**
- ❑ **Purpose of Workshop**
- ❑ **Summary**

Summary

- ❑ Proposed extensions to COCOMO for development of Secure Systems
 - Based on *Common Criteria for Secure Systems*
 - 1 Driver: SECU
 - 3 Factors:
 - Development for Security
 - Operational Security
 - Physical Security
 - Affects on other COCOMO II Drivers
 - RELY, CPLX, DOCU, SITE, TOOL
 - Affects Size
 - Affects project risk

Issues

- ❑ Do we have right COCOMO II drivers?
 - How many drivers should be defined?
 - Need further analysis of *Common Criteria*
- ❑ Need refined rating system
- ❑ Need Delphi for rating
- ❑ Need to analyze project data
- ❑ What's impact of Security on
 - Inception?
 - Transition?