Costing Secure Systems
Workshop Report

Edward Colbert
Danni Wu
{ecolbert, danwu}@cse.usc.edu

7th Workshop on Costing Secure Systems
Annual Research Review 2005
USC Center for Software Engineering

Goal Of Workshop

☑ Review proposed
  – Model for costing development of secure systems
  – Extensions to COCOMO II for development of secure software systems

☑ Feedback on behavior analysis
  – Validate proposed models
  – Identify research opportunities

☑ Review Delphi
  – For COCOMO Security Extension ("Nd2NOMO")

☑ Identify data sources
Outline

- Project Schedule
- Early Estimation Model
- COCOMO Security Extension ("Nd2NOMO")
- Delphi Collection Approach
- To Do

Cost Model for System Security Increment 1 (Feb – July ’04)

<table>
<thead>
<tr>
<th>Task Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop Early Estimation Model</td>
<td>Prototype model</td>
</tr>
<tr>
<td>2. Sources of Cost</td>
<td>Identify, define, scope sources of cost</td>
</tr>
<tr>
<td>3. Secure Product Taxonomy</td>
<td>Identify, define, scope product elements</td>
</tr>
<tr>
<td>4. COCOMO II Security Extensions</td>
<td>Refine model form and data definitions</td>
</tr>
<tr>
<td>5. COCOTS Security Extensions</td>
<td>Explore security aspects in COCOTS data collection</td>
</tr>
</tbody>
</table>
### Cost Model for System Security Increment 2 (Aug ’04 – July ’05)

<table>
<thead>
<tr>
<th>Task Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop Early Estimation Model</td>
<td>➢ Experimental use &amp; refinement</td>
</tr>
<tr>
<td>2. Sources of Cost</td>
<td>➢ Prioritize sources of cost needing CER’s</td>
</tr>
<tr>
<td></td>
<td>➢ Refine, prototype, experiment with top-priority CER’s</td>
</tr>
<tr>
<td></td>
<td>➢ Relate to scope of COCOMO II security extensions</td>
</tr>
<tr>
<td>3. Secure Product Taxonomy</td>
<td>➢ Experimental use, feedback, and refinement</td>
</tr>
<tr>
<td>4. COCOMO II Security Extensions</td>
<td>➢ Refine, scope, form, definitions based on results of Tasks 1-3</td>
</tr>
<tr>
<td></td>
<td>➢ Experimentally apply to pilot projects, obtain usage feedback</td>
</tr>
<tr>
<td>5. COCOTS Security Extensions</td>
<td>➢ Develop initial scope, form, definitions based on results of Tasks 1-4</td>
</tr>
</tbody>
</table>

### Cost Model for System Security Increment 3 (Apr ’05 – Sep ’06)

<table>
<thead>
<tr>
<th>Task Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop Early Estimation Model</td>
<td>➢ Evolution; integration with other models</td>
</tr>
<tr>
<td>2. Sources of Cost</td>
<td>➢ Refine sources of cost, CER’s based on usage feedback</td>
</tr>
<tr>
<td></td>
<td>➢ Integrate with other models</td>
</tr>
<tr>
<td></td>
<td>➢ Address lower-priority CER’s as appropriate</td>
</tr>
<tr>
<td>3. Secure Product Taxonomy</td>
<td>➢ Monitor evolution</td>
</tr>
<tr>
<td>4. COCOMO II Security Extensions</td>
<td>➢ Baseline model definitions</td>
</tr>
<tr>
<td></td>
<td>➢ Collect project data</td>
</tr>
<tr>
<td></td>
<td>➢ Develop initially calibrated model; experiment and refine</td>
</tr>
<tr>
<td>5. COCOTS Security Extensions</td>
<td>➢ Experimentally apply to pilot projects</td>
</tr>
<tr>
<td></td>
<td>➢ Refine, baseline based on usage feedback</td>
</tr>
</tbody>
</table>
Outline

- Project Schedule
- Early Estimation Model
- COCOMO Security Extension ("Nd2NOMO")
- Delphi Collection Approach
- To Do

Revised Formula for Cost of System & of Security

\[ C_{total} = C_{Initial/Mission Analysis} + C_{Investment Analysis} + C_{System Engineering} + C_{Dev & Imp} + C_{Sys of Sys Integration} + C_{Install/Deployment} + C_{O&M} + C_{Disposal} \]

\[ C_{Dev & Imp} = C_{Design & Build HW} + C_{Design & Build SW} + C_{Purchased Services} + C_{COTS-Sys} + C_{Env-Mods-design} + C_{Bus-Proc-Re-engineering} \]

\[ C_{total} \text{ (Security)} = C_{total} \text{ (with security)} - C_{total} \text{ (without security)} \]

\( C = \text{Cost} \)
### Formula Elements & COCOMO Family

<table>
<thead>
<tr>
<th>Formula Elements</th>
<th>COCOMO Family Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E_{\text{System Engineering}} )</td>
<td>COSYSMO (new)</td>
</tr>
<tr>
<td>( E_{\text{design &amp; build SW}} )</td>
<td>COCOMO-II</td>
</tr>
<tr>
<td>( E_{\text{Sys of Sys Integration}} )</td>
<td>COCOTS</td>
</tr>
<tr>
<td></td>
<td>COSoSIMO (new)</td>
</tr>
</tbody>
</table>

### Cost Model for Secure System Approach

- Identify major sources of cost
  - To
    - Develop
    - Own
  - Including
    - Facilities
    - Equipment
    - People
    - Acquired Systems
    - Services
How to Estimate Costs?

- Costing Approaches
  - Activity Models
  - Unit Costing
  - Analogy Base
  - Parametric

- For each source of cost, identify appropriate means
  - Cost Estimation Relation (CER)

Cost Estimation Relations (CER) Example

<table>
<thead>
<tr>
<th>Sample Activity</th>
<th>Preparation for Training</th>
<th>Classroom Training</th>
<th>Periodic Training on new procedures</th>
<th>Software Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>CER</td>
<td>Activity-based</td>
<td>Unit costing</td>
<td>Analogy-based</td>
<td>Parametric</td>
</tr>
<tr>
<td>Rule</td>
<td>10-20 hours for each Class Hour</td>
<td>N trainers total M trainees</td>
<td>It cost us $XXX last year,…</td>
<td>COCOMO II</td>
</tr>
</tbody>
</table>
FAA Acquisition & Standard WBS

- Analyzed FAA WBS to identify where security will affect activities
  - David Seaver pointed out not clear where security issues related to data management fit

- Started study of Standard WBS

2nd Prototype Tool for Early Estimation of System Development Cost (1 of 2)

- Currently version relatively basic
- Allows user to:
  - Estimate system development cost based on WBS
    - Enter cost at any level of WBS
      - Currently manual entry of WBS activities below 1st level
    - Enter any number of cost factors associated with WBS level
      - Use any CER
        » Activity-based
        » Unit cost
        » Analogy
        » Parametric
    - Sums costs
2nd Prototype Tool for Early Estimation of System Development Cost (2 of 2)

- Allows user to (cont.):
  - Estimate top-level WBS activity cost based on total cost
    - Enter total
    - Tailor distribution percentages
    - Computes top-level
  - Creates DB of entered data
  - Exports to Excel spreadsheet
1st Prototype Tool Screenshot#2
Advance Estimate — Cost Item By Analog

1st Prototype Tool Screenshot#3
Advance Estimate — Cost Item By Parametric Models
1st Prototype Tool Screenshot#4
Advance Estimate — Cost item by Unit/Activity Cost

2nd Prototype Tool for Early Estimation of System Development Cost (cont.)

- Plans
  - Add detail WBS activities
  - Add suggested cost factors

- Tool may also be useful for collecting data from projects
Outline

- Project Schedule
- Early Estimation Model
- COCOMO Security Extension ("Nd2NOMO")
- Delphi Collection Approach
- To Do

Effect Of Security On COCOMO II

- Source lines of code (SLOC’s) increased
  - Implementation of Security Functional Requirements (SFR’s)

- Effort to produce code increased by
  - Security Assurance Requirements (SAR’s)
  - A few Security Functional Requirements (SFR’S)

- Effort for “outer phases” of life–cycle (e.g. Inception, Transition) increased by
  - Additional documents
  - Additional activities
    - e.g. definition of security roles, certification
Effect Of Security Functional Requirements On SLOC’s & Computed Effort (cont.)

- 2 sources of change
  - Code for Security functions
    - Many systems add separate trusted software component(s)
      - e.g. Security Manager or Authorization & Access-Administrator
    - Common Criteria calls Target of Evaluation (TOE) Security Functions (TSF)
  - Code added to core application (non–TSF)
    - Authorization & access checks, error messages, etc.

Computation of total effort

\[ P_{\text{total}} = P_{\text{TSF}} + P_{\text{application}} \]

- TSF often developed at higher level of security
Affect Of Security On Effort to Produce SLOC’s

- Generally increased by
  - Security Assurance Requirements (SAR’s)
  - A few Security Functional Requirements (SFR’S)
    - e.g. log requirements may increase STOR value

Effort increase treated as COCOMO multiplicative driver

- TSF typically relatively small part of system code
  - Any exponential effects relatively minor
    - Can approximate as linear (multiplicative)
    - Non-linear effects may be captured by affect of security on existing COCOMO scale factors

- Non-TSF developed at lower security levels
  - Any exponential effects can be approximated as linear (multiplicative)
    - Possible exception CC assurance requirements apply to whole TOE
Analysis of SFR’s Effect on Existing COCOMO Drivers

- Determined which COCOMO driver effected by each SFR
  - Currently treating all as equal effect
  - Differentiating seems like too detailed for model
    - Not likely to be able to differentiate so finely
    - Nobody is likely to want to specify so finely

<table>
<thead>
<tr>
<th>Common Criteria SFR's</th>
<th>COCOMO Drivers</th>
<th>MULTI</th>
<th>SCALE</th>
<th>PRED</th>
<th>FIRE</th>
<th>PLEX</th>
<th>TOOL</th>
<th>SITE</th>
<th>SEC</th>
<th>Drivers Affected</th>
<th>Total COCOMO Drivers Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU</td>
<td>ARP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DEHS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SAA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SEL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>STG</td>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FCO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

D = direct, I = indirect

Effect Of Security Assurance Requirements On Effort to Produce SLOC's

- 1 driver (SECU) that addresses most SAR's (& relevant SFR's)
  - Based on 3 factors
    - "Development" SAR's
    - Independent Test & Certification
    - Development Process Constraints
  - Derived from Common Criteria & industry best practices

- Guidelines for levels on existing COCOMO II drivers
  - Some Development SAR’s overlaps with some existing drivers e.g. Reliability (RELY), Documentation (DOC)
  - Don't want to double count effect

- Special consideration of Independent Test & Certification
Analysis of Security Assurance Requirements
Effect on Existing COCOMO Drivers

- Determined which COCOMO driver effected by each SAR
- Organized SAR’s by CC Evaluation Assurance Levels (EAL’s)
- Developed guide for
  - Selection of levels for some drivers
    i.e. RELY, DATA, CPLX, DOCU
  - Suggested levels for drivers that introduce risk if not met
    i.e. PMAT & Tool
    e.g. insufficient Process Maturity when desired assurance >= high

<table>
<thead>
<tr>
<th>EAL</th>
<th>Scalars</th>
<th>RELY</th>
<th>RESL</th>
<th>DATA</th>
<th>DOCU</th>
<th>TOOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Nominal</td>
<td>Nominal</td>
<td>Nominal</td>
<td>Nominal+</td>
<td>Nominal</td>
<td>Nominal</td>
</tr>
<tr>
<td>2</td>
<td>Nominal+</td>
<td>Nominal+</td>
<td>Nominal</td>
<td>Nominal</td>
<td>Nominal</td>
<td>Nominal</td>
</tr>
<tr>
<td>3</td>
<td>Nominal</td>
<td>High+</td>
<td>High</td>
<td>Nominal+</td>
<td>High</td>
<td>Nominal+</td>
</tr>
<tr>
<td>4</td>
<td>Nominal</td>
<td>High+</td>
<td>High</td>
<td>Nominal+</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Nominal+</td>
<td>High+</td>
<td>High</td>
<td>High+</td>
<td>High+</td>
<td>High+</td>
</tr>
<tr>
<td>6</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>7</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

- For TOOL & PMAT
  - Set level to actual for developing organization
  - Project risk if developer’s level not at least suggested level
Effects of Independent Test & Certification SAR’s

- Developer support effort, if any, is part of SECU
  e.g. preparation TOE for delivery to independent certifier?

- Certifier’s cost adds to either
  - Acquisition cost of customer, if custom application
  - Developer’s cost, if “Shrink Wrap” products sold to government
    • e.g. Firewall

- Certifier’s time adds to project schedule

- If estimating maintenance cost,
  - Calculate development effort for change
    • Except testing
    - Must test whole
  - Calculate certifier’s cost on complete TOE size
**New Security Driver (SECU)**

- Derived from Common Criteria & industry best practices
  - Based on 3 factors
    - Development SAR's
    - Independent Test & Certification
    - Development Process Constraints
- COCOMO Driver Ratings
  - Nominal (Nom)
  - High (HI)
  - Very High (VH)
  - Extremely High (XH)
  - Super High (XXH)
  - Ultra High (XXXH)

**COCOMO Driver Ratings**

- Nominal (Nom)
- High (HI)
- Very High (VH)
- Extremely High (XH)
- Super High (XXH)
- Ultra High (XXXH)

**New COCOMO Levels**

- 6 COCOMO levels ≈ 7 CC EAL’s (or equivalent activity)
  - Treating EAL 1 as Nominal & EAL 2 as Nominal+50 (or High-50 😊)
  - Tailoring/Modification/Addition of SAR’s handled by increasing/decreasing base level

<table>
<thead>
<tr>
<th>Rating Level</th>
<th>Estimated Multiplies</th>
<th>Rating Scale (Refer to Supplement for details)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal (NOM)</td>
<td>1.00</td>
<td>No security requirements of added protection</td>
</tr>
<tr>
<td>High (HI)</td>
<td></td>
<td>Informal security requirements, methodically tested and checked</td>
</tr>
<tr>
<td>Very High (VH)</td>
<td></td>
<td>Methodically designed, tested and checked</td>
</tr>
<tr>
<td>Extra High (XH)</td>
<td></td>
<td>Semi-formally designed and tested</td>
</tr>
<tr>
<td>Super High (XXH)</td>
<td></td>
<td>Semi-formally verified designed and tested</td>
</tr>
<tr>
<td>Ultra High (XXXH)</td>
<td></td>
<td>Formally verified designed and tested</td>
</tr>
</tbody>
</table>
Example of COCOMO Estimation with Security

Assume:

- Application 1000 KSLOC SECU (App) = Nominal
- Trusted SW 10 KSLOC SECU (TSF) = High
- SF = 1
- All Multipliers (except Security) = 1 (Nominal)

SECU Values

- Nominal = 1
- High = 2
- VH = 3
- EH = 4
- SH = 6
- Strat = 7

Then

\[ PM \text{ (dev)} = PM \text{ (Trusted)} + PM \text{ (App)} = 2.94 \times ((10 \times \text{SECU(Trusted)}) + (1000 \times \text{SECU(App)})) = 2.94 \times ((10 \times 2) + (1000 \times 1)) = 2.94 \times 1020 \]

Effort in Person Month

\[ PM_{\text{estimated}} = A \times (\text{Size})^{SF} \times \prod EM_i \]

SF: Scale Factors (5) EM: Effort Multipliers (17)

Security Effects on Effort for “Outer Phases”

- Protection Profile (PP) capital investment or overhead
- Security Target (ST) definitions & verification add to upfront activities
  - Increase Inception Phase effort %
  - Possibly increase Investment & Mission Analysis
Security Effects on Effort for “Outer Phases” (cont.)

- Independent test & certification SAR’s add to schedule & cost
  - May increase
    - Transition Phase cost
    - Schedule independent of development effort

- Maintenance & independent certification SAR’s add to maintenance effort
  - Need slightly different calculation from standard COCOMO approach

Using SFR’s to Estimate Size

- Issue from last workshop:
  - Lot’s of SFR’s
  - No defined levels
  - Can’t
    - Ask about all SFR’s individually to assess affect on size
    - Get enough data about all SFR’s individually to analyze

- Need to simplify

- Analyzed registered Security Targets (ST)
What’s in Security Target Specification

- TOE scope & description
- TOE security environment
  - Security assumptions
  - Threats
  - Organization security policies
- Security objectives
- Security requirements
  - SFR
  - SAR
  - IT environment security requirements
- TOE summary
- Rational for
  - Security objectives, SFR, SAR
  - Explicitly stated security requirements
  - SFR and SAR dependencies

Analysis of Security Targets

- 149 Security Target(ST) Files
  - From http://niap.nist.gov
  - EAL range 1-4
    - Some modified
  - From different countries
    - US, Canada, German, England, Australia
    - French just added in
  - From different domains
    - OS, Firewall, IDS, Network Management, Sensitive Data Protection, Trusted DBMS, VPN, etc.
  - From different companies
    - Including Microsoft, IBM, Cisco, Sun, Symantec, McAfee, etc.
New Treatment of SFR’s Sizing

- Were looking at frequency of use in ST’s
  - Daniel Faigin (Aerospace Corp.)
    - Advised can’t rely on for costing
    - Agreed can be useful guide for new projects
    - Suggested alternative sizing
New Treatment of SFR’s Sizing (cont.)

- Define 3(+1) SFR size categories
  - Based on SFR components’ effect on TSF code size
    - Low
      - Adds few SLOCS
    - Medium
      - Adds moderate SLOCS
    - High
      - Adds many SLOCS
    - Undetermined
      - ST sensitive
      - Cannot be estimated without project implementation details

New Treatment of SFR’s Sizing (cont.)

- Assign SFR components to size categories
  - For undetermined, look at customize form in ST’s
- Determine approximate size for each SFR
  - Gather size data from companies that registered ST’s
  - Category by solving equations
    \[
    \text{TSF Size} = \left(\#\text{lows} \times \text{size-low}\right) + \left(\#\text{mediums} \times \text{size-medium}\right) + \left(\#\text{highs} \times \text{size-high}\right)
    \]

<table>
<thead>
<tr>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Undetermined</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU</td>
<td>GEN1, SAR1, SAR2</td>
<td>GEN2, SAA1, SAA3, SAR3, SEL1, STG1, STG3</td>
<td>SAA2, SAA4, STG2, STG4</td>
</tr>
<tr>
<td>FCO</td>
<td>****</td>
<td>***</td>
<td>***</td>
</tr>
</tbody>
</table>

© 2002-5 USC-CSE 48 16 March 2005
New Treatment of SFR’s Sizing (cont.)

- New project computes size by
  - Determine SFR’s
    - Inc. customized “undeterminable” SFR’s
  - Count SFR’s in each size category
  - Calculate TSF size
    
    \[
    \text{TSF Size} = \\
    (#\text{lows} \times \text{size-low}) + (#\text{mediums} \times \text{size-medium}) + \\
    (#\text{highs} \times \text{size-high})
    \]

Additional Issues Affect Sizing Estimate

- 35 out of 125 ST’s extend CC-define SFR’s
  - Only a few extensions per ST
  - Probably insignificant
  - May need to adjust cost driver to account for custom SFR’s

- Some SFR components used multiple times in some ST’s
  - e.g. User Authentication for remote login & local login
  - Need to avoid double counting during cost estimation
    
    \[
    \text{TSF Size} = \text{cost to develop plus cost to reuse}
    \]
Benefits of New Treatment SFR’s Sizing

- **Simplify Delphi**
  - Effort from researcher to put SFR’s into different categories
  - Experts
    - Advise/confirm category assignment
    - Estimate approximate sizes for categories?

- **Feasibility of calibration**
  - Only input from developers is ST & total TSF SLOC
  - Few variables
    - 3(+1) size categories
    - Reuse factor

Benefits of Categorizing SFR components (cont.)

- **Addresses SFR customizations**
  - Assignment, selection & iterations
    - User needs to determine reuse factor for iteration

- **Related to ST but not totally depend on**

- **Related to CC but not totally depend on**

- **Scalable**
  - User-custom just need to be assigned to size category

- **Evolvability**
  - SFR categories not likely to change dramatically due to new version of CC
Analysis of ST Summary

- 149 Registered Secret Targets (ST)
  - EAL’s range 1-4
  - Identified frequency of SFR’s
    - Not shown
    - Only eight ST’s include Privacy (FPR)
      - Have we missed domain that use FPR?
        » Financial Systems?
  - Identified frequency of SF Classes
  - Identified new TSF sizing approach

- Additional variations result from
  - Custom requirements

Nd2NOMO Prototype 1

- Building into COCOMO II Spreadsheet
Side Benefit of Analysis: Selecting Security Requirements for Products

- Analysis of ST can be
  - Specific guide for Domains with registered ST’s
  - Generally guide for other domains
    • e.g. frequently used requirements

- We’ve previously analyzed SAR’s & SFR’s for product security objectives
  - See next page
  - Need to compare to ST’s

Map Security Objectives with Common Criteria

<table>
<thead>
<tr>
<th>Common Criteria</th>
<th>Security Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Family</td>
</tr>
<tr>
<td>Security Audit</td>
<td>Authorization</td>
</tr>
<tr>
<td>(PAU)</td>
<td>Identity Management</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td>Recoverability</td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>ARP</td>
<td>X</td>
</tr>
<tr>
<td>GEN</td>
<td>X</td>
</tr>
<tr>
<td>SAR</td>
<td>X</td>
</tr>
<tr>
<td>SEC</td>
<td>X</td>
</tr>
<tr>
<td>STG</td>
<td>X</td>
</tr>
<tr>
<td>NBO</td>
<td></td>
</tr>
<tr>
<td>NBR</td>
<td></td>
</tr>
<tr>
<td>Cryptographic Support (FCS)</td>
<td></td>
</tr>
<tr>
<td>COM</td>
<td>X</td>
</tr>
<tr>
<td>COP</td>
<td>X</td>
</tr>
<tr>
<td>User Data Protection (FDP)</td>
<td></td>
</tr>
<tr>
<td>ACC</td>
<td>X</td>
</tr>
<tr>
<td>ACF</td>
<td>X</td>
</tr>
<tr>
<td>SAM</td>
<td>X</td>
</tr>
<tr>
<td>STG</td>
<td></td>
</tr>
<tr>
<td>TRC</td>
<td></td>
</tr>
<tr>
<td>TIC</td>
<td>X</td>
</tr>
<tr>
<td>TIP</td>
<td>X</td>
</tr>
<tr>
<td>RIP</td>
<td>X</td>
</tr>
<tr>
<td>ROL</td>
<td></td>
</tr>
<tr>
<td>SDI</td>
<td></td>
</tr>
<tr>
<td>ITC</td>
<td>X</td>
</tr>
<tr>
<td>IFT</td>
<td>X</td>
</tr>
<tr>
<td>Identification &amp; authentication (FIA)</td>
<td></td>
</tr>
<tr>
<td>APD</td>
<td>X</td>
</tr>
<tr>
<td>SDS</td>
<td>X</td>
</tr>
</tbody>
</table>

Can help developers identify appropriate SAR’s & SFR’s
Basic Development Cost Estimation with Security Extension Process

- Determine applicable security objectives
  - Apply product taxonomy or security objects
  - Determine which objectives to be done in software

- Estimate
  - Size of trust software
  - Size increase of non-TSF software

- Determine
  - Required assurance level
  - Effort for TSF & non-TSF software
  - Effort for pre-elaboration (initial) work
  - Effort for transition, installation
    - Inc. independent certification

- Calculate total effort

COTS, Sizing, & Security Extension

- Uncustomized COTS
  e.g. Microsoft Windows, Oracle
  - Can treated as IT environment (or part of)
  - Issue: impact of SoS integration

- Building wrapper around COTS
  - Can treated as IT environment (or part of)
  - Integration (glue code) considered inside TOE scope
    - TSF or Non-TSF

- Customized COTS
  - Both reuse & integration considered inside TOE scope
    - TSF or Non-TSF
  - Need full documentation & testing
COTS, Sizing, & Security Extension (cont.)

- Maintenance issues
  - New patches
  - Technology update
    - 9 months for new release
  - Re-certification needed

Outline

- Project Schedule
- Early Estimation Model
- COCOMO Security Extension ("Nd2NOMO")
- Delphi Collection Approach
- To Do
Draft Delphi Structure

- Question Sections
  - Increased Code Size for Security Functional Requirements (SFR's)
    - TSF Code
    - Application (Non-TSF)
  - Increased Effort & Schedule to Produce Secure Code
    - Adjustments to Current COCOMO Effort Drivers based on SFR's & SAR's
    - Increased Effort Due to Security Assurance Requirements (SAR's)
    - Increased Effort & Schedule Due to Security Independent Test & Certification SAR's
    - Increased Effort Due to Development Process Constraints
  - Adjustments to effort to do other Phases of Life-Cycle for Security Software Systems

Outline

- Project Schedule
- Early Estimation Model
- Work-Breakdown Structure (WBS)
- Common Criteria & Security Objectives
- COCOMO Security Extension ("Nd2NOMO")
- Delphi Collection Approach
- To Do
To Do

- Create website
- Create Nd2NOMO prototype in DBA-COCOMO
- Refine Secure System costing prototype
- Get more feedback from security community
- Refine models
- Refine Delphi
- Collect & analyze data
- Write Papers & Ph.D. Thesis (theses?)

New USC CSE Security Team