Costing Secure Systems
Workshop Report

Edward Colbert, Dan Wu,
Scribe: Alex Lam
{ecolbert, alexankl}@cse.usc.edu,
danwu@usc.edu

18th Annual COCOMO II & Software Costing Forum
2003
Participants

- Ed Colbert, USC, Moderator
- Danni Wu, USC, Assistant Moderator
- Alex Lam, USC, Unpaid scribe 😊
- Don Reifer, USC (don@reifer.com)
- George Huling, USC (g.huling@alumni.duke.edu)
- Paul Spelling, Aerospace Corp. (stelling@aero.org)
- LiGuo Huang, USC (liguohua@usc.edu)
- Clate Stansbury, MCR (cstansbury@mcri.com)
- Anca-Jiliana Stoica, RIT (anca@dsv.su.se)
- Ernie Lucier, FAA (ernest.lucier@faa.gov)
- Suzanne Williamson, Raytheon (suzannes_Williamson@raytheon.com)
- Linda Laird, Stevens Tech (Linda_m_laird@msn.com)
Outline

- Highlights
- Most Promising Opportunities
- Model Refinements
- Most Critical Issues
- Research Areas
- To Do
Don gave security tutorial

Ernie presented “A New Look at Cyber Defense”
   – By Art Pyster, Deputy Assistant Administrator for Information Services and Deputy Chief Information Officer

Ed reviewed USC’s
   – Plans
   – System Security Model
   – COCOMO II Model

Discussion
   – Lively participation
The “Android” Cyber Defense – Emulates most resilient system in world
– From “A New Look at Cyber Defense”
Most Promising Opportunities

- System Estimation Model
  - Suzanne “Excellent Job”

- Threat Analysis Impact on System (M-H, L-M*)
  - Different type threats → different solutions → Diff development cost
    - e.g. Prevention vs. Recovery/Response
  - Taxonomy of threat types will be high payoff
  - Linda thinks typical analysis will probably show 80/20 rule

- Understanding Meaning of High Availability (H, L)
  - Availability is separate issue from Security
  - Could have system w/ low availability; but high security requirement

*Payoff, Difficulty
Model Refinements

- **COCOMO**
  - Review drivers for overlap security impact (H,L)
    - e.g.
      - SITE ➔ Collocation & Communication each affected
      - PVOL ➔ Platform changes affected
  - COCOTS
    - Trade off buy & wrap verses build
    - Issue: 9 month ave. release of COTS update

- **Secure Process (H, H)**
  - Issue:
    - How good is process for developing secure system?
    - How good is process for operating secure system?

- **Agile security approaches? (L, M-H)**
Model Refinements (cont.)

What’s distribution for full system?

- Mission/Investment Analysis
- Elaboration
- Construction
- Transition 1+ systems*
- Y1 O&M
- Y2 O&M

* Installation costs are highly dependent on # systems
Most Critical Issues

☐ Verify process steps delivers value to product (H, H)
   – FAA Security Certification & Accreditation Packages (SCAP) defines long & expensive process
     • What’s value of steps?

☐ Missing relations to other drivers (H, L)
   – PCAP & ACAP
     – Programmers & Designers need security knowledge
Research Areas

- Add security to legacy systems (H, H)

- Secure Architecture patterns (M-H, L-M)
  - Security sensitive?
  - Oodles of fun

- Trade off Analysis Tool (H, M-H)
Characterization of system

<table>
<thead>
<tr>
<th>Mode of Op</th>
<th>Protect Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand alone</td>
<td></td>
</tr>
<tr>
<td>Dedicated</td>
<td>Authentication</td>
</tr>
<tr>
<td>Sys High</td>
<td>Sec Level / EAL</td>
</tr>
<tr>
<td>Controlled</td>
<td>Sec Level / EAL</td>
</tr>
<tr>
<td>MLS</td>
<td>Sec Level / EAL</td>
</tr>
<tr>
<td>Networked</td>
<td></td>
</tr>
<tr>
<td>Dedicated</td>
<td>Sec Level / EAL</td>
</tr>
<tr>
<td>Sys High</td>
<td>Sec Level / EAL</td>
</tr>
<tr>
<td>Controlled</td>
<td></td>
</tr>
<tr>
<td>MLS</td>
<td></td>
</tr>
</tbody>
</table>
To Do

- Create website
- Behavior Analysis
  - Commercial
  - Security community
- Refine models
- Create Delphi
- Collect & analyze data
- Write Ph.D. Thesis (theses?)