Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

MAY 12, 2023
Sam Procter
Document Markings

Copyright 2023 Carnegie Mellon University.
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation. NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu. DM23-0475
Agenda

• Effects-Based Reasoning
• Guidewords
• Speaking the Language of Security
Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Effects-Based Reasoning
Effects-Based Reasoning
History and Explanation

“The CFEM organizes diverse fault categories into a cohesive framework by classifying faults according to the effect they have on the required system services rather than by targeting the source of the fault condition.”


Usage
• Aligns well with top-down analyses
• Used by AADL’s EMV2 library

What
• Number of error causes are unbounded and may be unknowable
• Error’s effects are (commonly) statically determinable and tightly bounded
Effects-Based Reasoning

Error *causes* are effectively unbounded, error *effects* can be bounded

Why

- Merges safety and security concerns
  - … does it matter *why* an input is malformed?

- Reduces analysis space*
  - * barring pathological errors

- Increases compositionality / locality
  - Does it matter *who* sent malformed input?

- Reduces ambiguity

- Better aligns with formal methods
  - Provides a notion of completeness, cf “Assumption Synthesis"

---


Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Guidewords
The Role of Guidewords

Guidewords are:

- “Baked into” many popular hazard analyses
- Fairly intuitive / don’t require a great deal of training
- Also conceivable as a taxonomy (Avižienis, Laprie) or attacker model (Dolev-Yao)

Guidewords used in hazard analysis help dictate the failure modes considered by analysts
# Guideword Comparison

<table>
<thead>
<tr>
<th>Concept</th>
<th>Avižienis et al</th>
<th>STPA</th>
<th>Dolev-Yao</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Message</td>
<td>Early Arrival</td>
<td>Providing</td>
<td>Craft New &amp; Send</td>
</tr>
<tr>
<td>Late Message</td>
<td>Late Arrival</td>
<td>Late</td>
<td>Delay</td>
</tr>
<tr>
<td>High Value</td>
<td>Value High</td>
<td>None*</td>
<td>Modify Existing</td>
</tr>
<tr>
<td>Low Value</td>
<td>Value Low</td>
<td>None*</td>
<td>Modify Existing</td>
</tr>
<tr>
<td>Service Stop</td>
<td>Halted</td>
<td>Fails to Provide</td>
<td>Drop</td>
</tr>
<tr>
<td>Babbling Idiot</td>
<td>Erratic</td>
<td>Providing</td>
<td>Craft New &amp; Send</td>
</tr>
<tr>
<td>Confidentiality Violation</td>
<td>[In security attributes]^</td>
<td>None</td>
<td>Read</td>
</tr>
</tbody>
</table>

---


^ confidentiality is present as a security attribute, Procter et al used dependability attributes exclusively.


* added in subsequent work

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Speaking the Language of Security
“At the heart of both safety engineering and security engineering lie decisions about priorities: how much to spend on protection against what.”

It is the hierarchical structure and organization that I argue:

- Safety can offer security
- Should bind the approaches
- Safety experts should focus on when communicating with security experts
“Lessons from Safety-Critical Systems”

Principles

• Guide the system to a safe state when things go wrong
• In an emergency, keep the information presented simple
• Pay attention to fault masking

Safety Analyses Can…

• Identify safe states
• Present information in a human-/user-centered way
• Detect opportunities for fault masking

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Sam Procter
sprocter@sei.cmu.edu