Cofer, Darren D **Collins**

From: IEEE Security & Privacy <onbehalfof@manuscriptcentral.com>
Sent: Wednesday, January 26, 2022 1:07 PM
To: Cofer, Darren D Collins; Amundson, Isaac E Collins; Babar, Junaid Collins; Hardin, David S Collins; Slind, Konrad L Collins; palexand@ku.edu; hatcliff@ksu.edu; robby@ksu.edu; gerwin.klein@proofcraft.systems; corey.lewis@unsw.edu.au; egm@cs.byu.edu; john.shackleton@adventiumlabs.com
Cc: security@computer.org; sp-eic@computer.org
Subject: [External] IEEE Security & Privacy, SPSI-2021-11-0255 - minor revision required

Follow Up Flag: Follow up
Flag Status: Flagged

IEEE Security & Privacy ,SPSI-2021-11-0255
manuscript type: SPSI: May/June 2022: Formal Methods at Scale
"Cyber Assured Systems Engineering at Scale"

Dear Dr. Darren Cofer,

After examining the reviews and the associate editor's recommendation, the editor in chief has decided that the manuscript needs minor revisions. It is necessary for you to address all relevant comments and provide justification if you disagree with a reviewer's assessment.

We are on a very tight schedule for this issue. Please submit your revision by February 4.

I have attached below the comments of the Associate Editor and the reviews.

Please maintain our 6,000–word limit as you make your revisions.

Please upload your revision and summary of changes, log on to https://mc.manuscriptcentral.com/sp-cs, click on your Author Center, click on "Manuscripts with Decisions." Under column named "Actions," click on "Create a Revision" next to the above manuscript number.

Also, highlight the changes to your manuscript within the document by using the track changes mode in MS Word or by using bold or colored text.

When submitting your revised manuscript, you will be required to respond to the comments made by the reviewer(s) in the space provided. Also, please document any changes you made to the original manuscript.

If you have any questions regarding our policies or procedures, please refer to the magazines' Author Information page, https://www.computer.org/web/peer-review/magazines, or feel free to contact me.

We look forward to receiving your revised manuscript.

Regards,

Mr. Dustin Martinez
Administrator
IEEE Security & Privacy

****

Associate Editor comments

Editor
Comments to Author :
Thank you for your submission. Please see the reviewers comments. Please address the comments and prepare a revision for submission. We are on a very tight schedule.
Please provide your revision by February 4.

Reviews:
Please note that some reviewers may have included additional comments in a separate file. If a review contains the note "see the attached file" under Section III A - Public Comments, you will need to log on to ScholarOne Manuscripts to view the file. After logging in, select the Author Center, click on the "Manuscripts with Decisions" queue and then click on the "view decision letter" link for this manuscript. You must scroll down to the very bottom of the letter to see the file(s), if any. This will open the file that the reviewer(s) or the Associate Editor included for you along with their review.

Reviewer: 1

Recommendation: Accept If Certain Minor Revisions Are Made

Comments:
The paper describes a set of tools that enable the formal analysis of a system specified using Architecture Analysis and Design Language (AADL). The tools incorporate, among other things, mechanisms for analyzing the cybersecurity of the system and developing cybersecurity requirements. The tools extend to the analysis of the designed and implemented system as well, so it's possible to assess whether the identified requirements are met by the implementation. The tools have been applied in the context of a design for an unmanned helicopter and in particular to modifying the design so that it incorporated a wireless tablet that could monitor data about nearby air traffic. By basing the architecture on the verified sel4 platform and applying various tools to assure first that the system specification meets its requirements and then that the implementation of the specific can be assured to conform to it, the project aims at the holy grail for high assurance systems, verification down to the code level.

The paper is reasonably clear and should be of interest to a broad audience. It reports a promising result -- that a team of development engineers, most of whom had no previous experience with formal methods, was able to use the tools effectively to meet the requirements of the demonstration. The parts of the paper describing the methodology and tools are quite detailed and might be improved by raising the level of the discussion a bit. Perhaps an overview describing at a high level the assurance argument for the entire system would eliminate the need for some of the detail. The account of the application, on the other hand, might benefit from additional detail, if available, about the training required (or not required) of the development teim, the time consumed in accomplishing the tasks involved, and so on.

The figures, with the exception of Figure 5, are barely legible in the pdf and will be illegible in print. Figure 4 is especially bad in this respect. They need to be redone, and possibly recast, so they actually add value to the paper. Also note that the description of Figure 1 asserts that the Planner module is white, but in fact, it's pink (and the reason for that is not explained).

Additional Questions:
1. How relevant is this manuscript to the readers of this periodical? Please explain your rating in the Detailed Comments section.: Very Relevant

2. To what extent is this manuscript relevant to readers around the world?: The manuscript is of interest to readers throughout the world

3. What is the most appropriate forum for the publication of this manuscript?: IEEE Magazine (general interest explanatory article with technical contributions)

1. Does the manuscript contain title, abstract, and/or keywords?: Yes

2. Are the title, abstract, and keywords appropriate? Please elaborate in the Detailed Comments section.: Yes

3. Does the manuscript contain sufficient and appropriate references (maximum 15-unless the article is a survey or tutorial in scope)? Please elaborate in the Detailed Comments section.: References are sufficient and appropriate

4. How would you rate the organization of the manuscript? Please elaborate in the Detailed Comments section.: Could be improved

5. Is the length of the manuscript appropriate for the topic? Please elaborate in the Detailed Comments section.: Satisfactory

6. Please rate and comment on the readability of this manuscript in the Detailed Comments section.: Readable - but requires some effort to understand

1. Please summarize what you view as the key point(s) of the manuscript and the importance of the content to the readers of this periodical.: The paper describes a set of tools that enable the formal analysis of a system specified using Architecture Analysis and Design Language (AADL). The tools incorporate, among other things, mechanisms for analyzing the cybersecurity of the system and developing cybersecurity requirements. The tools extend to the analysis of the designed and implemented system as well, so it's possible to assess whether the identified requirements are met by the implementation. The tools have been applied in the context of a design for an unmanned helicopter and in particular to modifying the design so that it incorporated a wireless tablet that could monitor data about nearby air traffic. By basing the architecture on the verified sel4 platform and applying various tools to assure first that the system specification meets its requirements and then that the implementation of the specific can be assured to conform to it, the project aims at the holy grail for high assurance systems, verification down to the code level.

2. Is the manuscript technically sound? Please explain your answer in the Detailed Comments section.: Appears to be - but didn't check completely

3. What do you see as this manuscript's contribution to the literature in this field?: It provides evidence that formal methods tools can be applied effectively by developers without special backgrounds and explains the specific tools and techniques used.

4. What do you see as the strongest aspect of this manuscript?: The example it provides.

5. What do you see as the weakest aspect of this manuscript?: Some of the description is perhaps overly detailed. See notes below. Most of the figures are likely to be illegible.

7. Please rate and comment on the timeliness and long term interest of this manuscript to S&P readers in the Detailed Comments section. Select all that apply.: Topic and content are likely to be of growing interest to S&P readers over the next 12 months

Please rate the manuscript. Explain your choice in the Detailed Comments section.: Good

Reviewer: 2

Recommendation: Accept If Certain Minor Revisions Are Made

Comments:
Overall, this was a really excellent paper that I enjoyed reading. The paper presents some great research which genuinely extends the limits, scale, and applications of formal methods technologies, fully meeting the brief for this special issue.

As stated above, I was really excited to read about such a range of formal methods tools, techniques, technologies, and verified components all used in one project, all contributing to a combined assurance case in a rigorous manner. This is a really important demonstration of how various tools can work together, and how outputs from different tools can be combined meaningfully to support the highest levels of assurance.

This paper presents low 'tech readiness level' research rather than finished products, so I think in reality it's unlikely that many avionics scenarios would be able to use the whole suite in such a comprehensive way for now. In spite of that, the presentation and combination of this array of tools is a fantastic piece of work, and strongly demonstrates the use of these formal methods tools at real-world, high-assurance scale.

Major comments:

I found it difficult to get the structure of the tool approach on first pass: this is a big toolset with lots of moving parts, and it required lots of effort on the part of the reader to construct a model of what each of the individual things do and how they work together. I would like to see some 'high level', introductory summary paragraph and/or graphic of how all the moving parts relate.

Some more transparency is needed over a couple of areas, specifically real-time requirements and programming language choices.
Although the BriefCASE toolset and workflow is not only targeted at avionics, the paper has a very strong avionics emphasis. In this light, much more consideration and discussion in the paper needed about domain-specific (avionics) requirements needed to address concerns.
For example, there is no meaningful discussion about real-time / WCET safety requirements in the avionics domain; RTOS is alluded to, and the 'Real-time scheduling' section starts to address this, but does not provide sufficient discussion about how these real-time safety critical requirements are met (or not) within the technologies used. This needs to be discussed more clearly (and should not be difficult to do so!), or I feel it will not be taken seriously by those in avionics.
Similarly, more discussion is needed about the apparent tension between the use of functional programming languages such as CakeML and the real-time/WCET requirements of the very conservative avionics domain (which would normally require manual memory management). The paper even mentions the JVM at one point (re: HAMR, p.9): I acknowledge that this output is not a core part of the toolset, but use of this in safety-related avionics context is seemingly implausible.

The paper would also benefit from a brief discussion about satisfaction of various safety standards. For example, there are supplements to DO-178C that cover MBSE, formal methods, and tool qualification: how does this approach relate to this or other relevant standards?

The paper should also make clear (Aircraft Application, p.12) whether the "vision processing module" that seL4 is running on is one for which seL4 is fully verified or not, i.e. is the VPM system's platform one for which the proofs are complete? I don't see it as a substantial problem if not, but transparency and clear descriptions over precisely what each element of verified technology (or analysis tool) does or does not buy the assurance methodology as a whole is essential to maintain trust in any approach.

Minor comments:

Figure 4 is blurry when zoomed in so can't see much of the assurance case
p.2, line 54, col 1 - "Proofs about models are meaningless unless..." - I appreciate the sentiment but it's a bit hyperbolic
p.4, "BriefCASE work flow": Where does your list of cybersecurity vulnerabilities come from? What is the threat model, and where does this come from?
p.4, "Requirements": At what layer or level are these vulnerabilities? How complete do you claim this approach is?
p.4, Section "Cyber Transforms" - Is there only one possible transform at each stage? If not what happens if there's more than one at any given stage? How did you choose this list of possible transforms, and what level of completeness do you believe you achieve with these transforms?
p.5, Source/citation needed for Lustre
p.6, line 43, col 1 - missing full stop after "contiguity types"
p.6, line 54, col 2 - "verified using Coq" - doesn't explain how
p.7, para 1: Does this attestation process only happen once, and then allow all messages (unauthenticated/unsigned) from that source? If so, how does the UAV know that message after this point aren't spoofed, replayed, or from another source? I assume there's some cryptographic protocol used here (creating an encrypted and/or authenticated channel), but this is not described.

Additional Questions:
1. How relevant is this manuscript to the readers of this periodical? Please explain your rating in the Detailed Comments section.: Very Relevant

2. To what extent is this manuscript relevant to readers around the world?: The manuscript is of interest to readers throughout the world

3. What is the most appropriate forum for the publication of this manuscript?: IEEE Magazine (general interest explanatory article with technical contributions)

1. Does the manuscript contain title, abstract, and/or keywords?: Yes

2. Are the title, abstract, and keywords appropriate? Please elaborate in the Detailed Comments section.: Yes

3. Does the manuscript contain sufficient and appropriate references (maximum 15-unless the article is a survey or tutorial in scope)? Please elaborate in the Detailed Comments section.: References are sufficient and appropriate

4. How would you rate the organization of the manuscript? Please elaborate in the Detailed Comments section.: Satisfactory

5. Is the length of the manuscript appropriate for the topic? Please elaborate in the Detailed Comments section.: Satisfactory

6. Please rate and comment on the readability of this manuscript in the Detailed Comments section.: Easy to read

1. Please summarize what you view as the key point(s) of the manuscript and the importance of the content to the readers of this periodical.: This paper presents and describes a comprehensive new approach to use of formal methods for large-scale, systems engineering assurance. This uses a 'model-based systems engineering' approach (and environment), integrating formal methods throughout, and across a range of different layers of the engineering design stack. This has the benefit of being able to rigorously address and mitigate a range of cyber-security issues at the design stage, rather than much later as is more usually the case. This paper demonstrates new combinations and use-cases for tooling, and shows the utility and possible scale of use-cases for formal methods-based analysis tools and techniques.

2. Is the manuscript technically sound? Please explain your answer in the Detailed Comments section.: Yes

3. What do you see as this manuscript's contribution to the literature in this field?: The combination of such an array of tools and verified components/technologies in this domain, into a genuinely comprehensive suite for high assurance evaluation is really impressive and a fantastic outcome. Combining this evidence together into formal-methods based reporting tools to build an all important assurance case completes the picture. Demonstrating that this can be done both at scale and in real-world systems is such a high impact indicator, and is something the field of formal methods needs substantially more of: well done.

4. What do you see as the strongest aspect of this manuscript?: The paper surveys a lot of potential tools; the authors have selected, identified, and constructed a complete workflow at a full life-cycle of high assurance product evaluation. This produces a coherent, focussed workflow, and all of the approaches are fit for purpose for their proposed context. The paper embeds evidence into the formal assurance case throughout, generating, documenting, and structuring the evidence for the assurance case. This results in a nice mixture of formal verification tools and techniques in combination with formally verified technologies and components, e.g., seL4 to achieve the required assurance levels.

5. What do you see as the weakest aspect of this manuscript?: Overall very good. However:
- Difficulty in navigation of the paper: the paper presents a big toolset with lots of moving parts; lots of effort on the part of the reader to construct a mental model of what each of the individual things do and how they work together. I would like to see some 'high level', introductory summary and/or graphic of how all the parts relate.
- The paper would benefit from more transparency over a couple of areas: please give more discussion about real time requirements and operating systems, and please give more discussion about programming languages and environments. See comments below for more detail.

7. Please rate and comment on the timeliness and long term interest of this manuscript to S&P readers in the Detailed Comments section. Select all that apply.: Topic and content are of immediate and continuing interest to S&P readers

Please rate the manuscript. Explain your choice in the Detailed Comments section.: Excellent