HARDEN: A High Assurance Design Environment

Haley Whitman, Michael Vai,
David Whelihan and Roger Khazan
MIT Lincoln Laboratory
Lexington, MA
Haley.Whitman@ll.mit.edu

Douglas Schafer
Air Force Research Laboratory
Rome, NY

Donald Russo
Booz Allen Hamilton
Rome, NY

***Abstract*—Systems resilient to cyber-attacks for mission assurance are difficult to develop, and the means of effectively evaluating them is even harder. We have developed a new architectural design and engineering environment, referred to as HARDEN (High AssuRance Design ENvironment), which supports an agile design methodology used to create secure and resilient systems. This new toolkit facilitates the quantitative analysis of a system's security posture by setting up a systematic approach of securing and analyzing embedded systems. HARDEN promotes the early co-design of functionality and security that now enables the development of mission assured systems.**

Keywords—cyber security; resiliency; design environment; requirement management

I. INTRODUCTION

Mission assurance, i.e. the verified belief that a system will complete its mission, requires that cyber-security and resilience of military systems be a first-class consideration along with functional requirements. Unfortunately, conveying a cyber-inclusive world-view to designers and architects of these systems has remained an elusive goal. The result is usually less-secure systems in which any security or resilience capabilities are bolted on as an after-thought. The central problem is that the creators of systems, the definers of mission goals, and experts on cyber-security do not speak the same language, or have any reasonable way of cooperating to provide systems that can meet mission goals despite an increasingly sophisticated cyber-adversary.

In order for all system stakeholders to effectively communicate, designers have to determine not only how system functions are to be developed, but also the pros and cons of using off-the-shelf hardware and software components. Choosing components based on performance and capabilities is relatively straightforward – developers already have plenty of tools and metrics (e.g., size, weight, power, and cost) to perform tradeoffs. In contrast, the evaluation of component security posture as they are being used in a system is still a problem. The problem is even more challenging as the use of secure components provides no guarantee to the security of the entire system as a whole.

We have recently created a mission assurance oriented embedded system design methodology [1], which leverage a cybersecurity metric to:

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Case Number 2018-0503, 2018 09 07, (Original Case Numbers: MSC/PA-2018-0269; 88ABW-2018-4224). This material is based upon work supported by the Dept. of the Air Force under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Dept. of the Air Force.

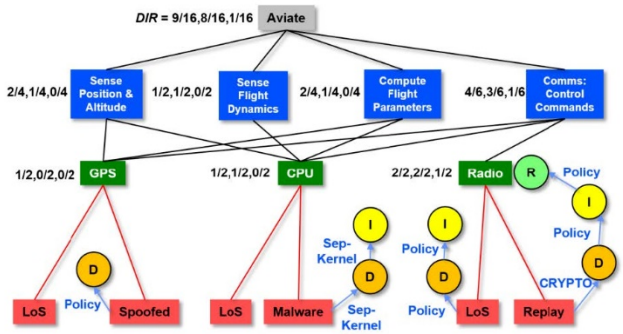

Fig. 1. Example of system analysis of an improved aviate function inside of an Auto-Pilot Module from a previous work [1].

- Tie functional and cybersecurity requirements together and facilitate their co-design at the early stage of system development.
- Quantifiably evaluate a system's security for design space exploration and design iterations.
- Determine the overhead caused by the addition of cybersecurity requirements and their return-on-investment (ROI).

An excerpt from an example of the systems analysis process in the Agile and Resilient Embedded Systems (ARES) design-for-mission-assurance approach is shown in Fig. 1. An overview of this methodology is given in Section II.

In this paper, we describe the development of a High Assurance Design Environment (HARDEN), which enables and automates the quantitative and documentation aspect of the ARES mission assurance analysis. HARDEN consists of a toolkit that complements existing requirement management tools used in system development (e.g. DOORS). By providing the means to attach proper traceability and tracking of development iterations this tool allows for developers and stakeholders to quantitatively determine and articulate ROI that was gained due to engineering decisions.

We have tested HARDEN and demonstrated its significant benefits in several development efforts, including the development of a secure processor [2] as well as the start for a new project involving the system security analysis for assurance of microelectronics [3]. We have found that existing system design tools such as Sparx Systems Enterprise Architect successfully track information regarding requirements and system specifications, but are not necessarily able to analyze and or built in a way to engineer a system with security in mind [3]. HARDEN finds its niche in a system's development by reuse information already tracked with these industry standard tools, and adding the ability to add to

established information with system vulnerabilities and defenses in mind. In doing so, a traceable impact is created and provided by HARDEN that may lead to significant strides towards real mission assurance for next generation systems.

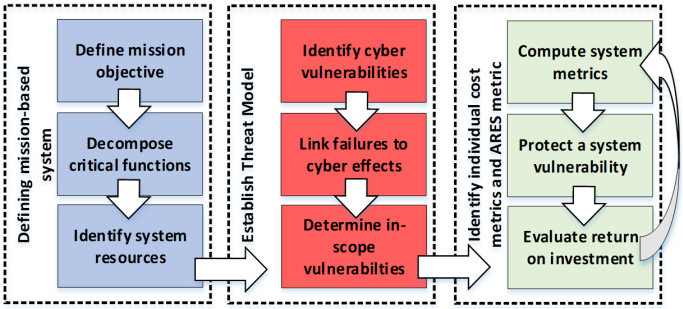

Fig. 2. The ARES process that HARDEN supports.

II. Overview of ARES

We will provide a few general concepts of the ARES methodology to facilitate our discussion. ARES focuses on differentiating two types of system protections, *hardening* and *resilience*. We define *hardening* as protections that are utilized to protect a system resource against particular attacks. On the other hand, *resilience* defines the measures that are capable of detecting that an attack is disrupting the system's mission objective. The resilience measure then isolates the attack from further spreading to other system resources, and resolves the threats by recovering necessary controls for the mission objective. These two principles are the basis of our top-down assessment approach in evaluating the mission assurance.

The ARES process for analyzing a system is shown in Fig. 2. First, a mission objective is identified for the system being analyzed. Using the system's CONOPS we then translate overall mission goals into a set of actions required for the successful mission operation, known as the Mission Essential Functions (MEFs). These MEFs are then mapped to the

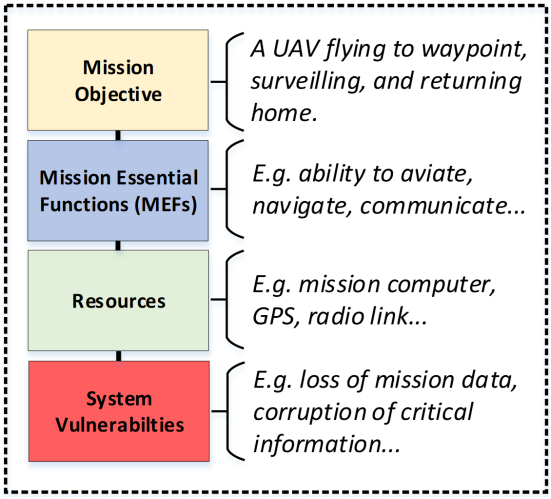

Fig. 3. The different HARDEN "objects" used for creating a hierarchy of a system architecture.

physical resources that will form the system. Examples of these types of engineering objects are found in Fig. 3. The ARES metric focuses on evaluating the cyber-induced effects that compromise the resources, and thus the MEFs, and tracks how this degrades the mission through a quantifiable metric by counting the number of cyber-effects against the system and how each threat is handled (i.e. through detection, isolation, and finally recovery).

III. Toolkit

HARDEN is designed to be easily adopted by typical engineering processes and facilitate the acquisition of a wide range of system types. The following design concepts and principles guided HARDEN's development

- Ease-of-use
- Ability to establish traceability (i.e. engineering decisions, versioning, and source material)
- Integrate into the engineering design process
- Ability to be system independent and adaptable.

The following engineered capabilities facilitate the above core concepts.

A. Diagramming

Diagramming system architectures is a core functionality of HARDEN. System architectures are input through a drag-and-drop or keyboard interface. Links between each of these nodes manage all entered engineering information in context of the larger system through custom data structures. The system graph is automatically organized and generated to display this information at a multiple abstraction levels intended for separate stakeholders.

B. Metric Calculations

The ARES quantitative metric is automatically updated and versioned on any engineering change to the system. New versions track the current safety and functional requirements to see if any additional system overhead still abides by the required threshold values spelled out in the requirement database.

C. Requirement Links

System functional, quality, and safety requirements are entered into HARDEN and attached to specific ARES objects (i.e. MEFs, Resources). Security related requirements attach to ARES objects and are comparable to the standard set of requirements for the requirement validation process. Requirements may be included through exports from industry standard tools, such as IBM® Rational® DOORS®.

D. Version and Change Tracking

All system iterations are versioned, and automated reports presenting a historical overview of each engineering change are available within the toolkit for analysis.

E. Security Library

HARDEN allows previously analyzed system components to be integrated into the analysis and architecture of new engineering efforts. We are currently testing the modularity of this functionality with MIT Lincoln Laboratory technology such as the Lincoln Open Cryptographic Management

Architecture (LOCKMA), which has been used in multiple defense-related projects [5].

F. *Analytical Documentation*

HARDEN generates system reports upon completion of an ARES diagram. These reports include graphs of the engineering changes over time, the ROI, the threat model, and other implementation details input into HARDEN. These reports aim to support the standard Joint Capabilities Integration and Development System (JCIDS) documentation efforts.

IV. Future Capabilities

Future development for HARDEN plans to include the following:

A. *Integrated Development Environment (IDE)*

1) Support the import functionality of several requirement management tools used by industry (e.g. IBM Rational DOORS [6]) by mapping system safety and functional requirements to the cybersecurity analysis. Cybersecurity requirements will be validated against existing system requirements for consistency.

2) Offer a plugin for a variety of IDEs (e.g. Eclipse, IntelliJ) to capture code documentation and other implementation details to attach to cybersecurity analysis.

B. *Training Materials*

1) Guided Tutorials and HARDEN help documentation will be provided to assist with the training and adoption of the ARES methodology onto new systems from new stakeholders.

C. *Security Suggestions*

1) Support for generated security improvements will be offered to existing designs. HARDEN will highlight areas of the analysis that would benefit the most from these features, maximizing the potential ROI for development work.

2) Offer the addition of a semantic modeling language (e.g. the Semantic Application Design Language [7]) that may be used to check requirements against the designed architecture models within HARDEN.

D. *Cyber Attack Modeling*

1) Support the analysis for modeling both specific attacks and system defense strategies and link these to the higher-level cyber vulnerabilities already defined in HARDEN.

V. Summary and Ongoing Work

The HARDEN tool, and the methodology it enables, bridges the gaps in the design process to integrate cyber-security and resilience into the world-view of system-designers. The most important contribution of HARDEN is that it provides a structure for an evidence-based approach to cyber-security and resilience, enabling the right technologies and techniques to be applied in the right places early in the design cycle. The result is mission specific quantifiable and testable assertions about improvements in cyber resilience. A snapshot of this tool examining the MEFs of an example mission is shown in Fig. 4.

This paper has presented our work on a toolkit used to facilitate a new method of analyzing and quantifying a system's cybersecurity development efforts. These efforts offers many advantages to current industry practices towards system development. MIT Lincoln Laboratory has seen some of these positive results of this methodology and assistive toolkit in previous work.

References

[1] D. Whelihan, M. Vai, et al., "Designing agility and resilience into embedded systems," MILCOM, 2017.

[2] M. Vai, D. Whelihan, J. Leemaster, H. Whitman, W. Wan, Y. Fei, R. Khazan, I. Lebedev, K. Hogan, S. Devadas, "Mission assurance: beyond secure processing," IEEE/CRE, 2018.

[3] M. Vai, D. Whelihan, R. Khazan, "Next-generation embedded processors: an update" GOMACTech, 2018.

[4] https://sparxsystems.com/, accessed 17 April, 2018.

[5] R. Khazan, D. Utin, "Lincoln open cryptographic management architecture," Technical Report DTIC Document, 2012.

[6] https://www.ibm.com/us-en/marketplace/rational-doors, accessed 17 April, 2018.

[7] http://sadl.sourceforge.net/, accessed 17 April, 2018.

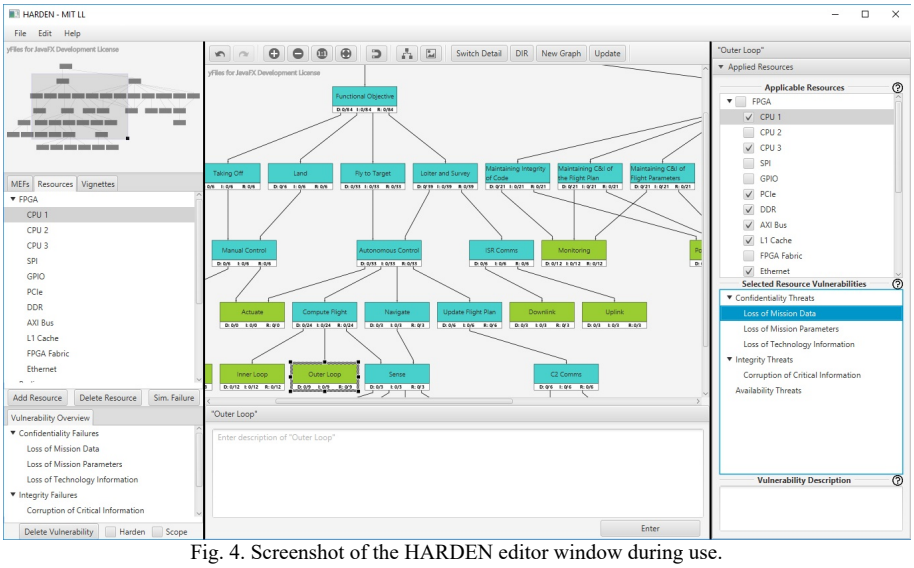

Fig. 4. Screenshot of the HARDEN editor window during use.