Tokeneer ID Station Project Case Study

Nancy R. Mead

April 2021

Tokeneer ID Station Project Case Study

Background

In order to demonstrate that developing highly secure systems to the level of rigor required by the higher assurance levels of the Common Criteria is possible, the NSA (National Security Agency) has asked Praxis High Integrity Systems to undertake a research project to develop part of an existing secure system (the Tokeneer System) in accordance with Praxis' own Correctness by Construction development process, a high-integrity process developed by Praxis and applied by them on a number of commercial projects. This development work will then be used to show the security community that it is possible to develop secure systems rigorously in a cost effective manner.

Although the Common Criteria and its forerunners (the ITSEC scheme, the TCSEC — Orange Book, and others) have been in existence for a considerable time, there has been less use of them by industry than desired by their developers. Part of the reason for this may be that industry do not believe that it is possible to develop systems to the higher levels of certification in a cost-effective manner. Our experience at Praxis High Integrity Systems is that systems can be developed rigorously, and that this yields both a high-quality system, and lower cost.

This development and research work has now been made available by the NSA to the software development and security communities in an effort to prove that it is possible to develop secure systems rigorously in a cost-effective manner.

Process

The development process applied to the Tokeneer ID Station high-integrity development can be summarised in terms of the following key phases:

- Requirements analysis (the REVEAL® process)
- Formal specification (using the formal language Z)
- Design (formal refinement of the specification and the INFORMED process)
- Implementation in SPARK Ada
- Verification (using the SPARK Examiner toolset)
- Top-down system testing

Project Findings

The Tokeneer ID Station development project has demonstrated that the Altran Correctness by Construction development process is capable to produce a high quality, low defect system in a cost effective manner following a process that conforms to the Common Criteria EAL5 requirements. The Tokeneer ID Station system's key statistics are:

- lines of code: 9939
- total effort (days): 260
- productivity (lines of code per day, overall): 38
- productivity (lines of code per day, coding phase): 203

- defects discovered since delivery: 4

With the aim of achieving EAL5 levels of assurance, we believe that the Correctness by Construction process can achieve EAL7. The proof activity we use in our Correctness by Construction process is sufficient for EAL7, which involves tool supported code proof but manual proof of the Specification and Design. The process can be tightened appropriately to meet the additional quality control requirements of EAL7 by using tools that provide fully integrated electronic support.

Case Study Overview

The key objective of this project was to obtain evidence of the applicability of the Praxis development process to EAL5-level system development. This includes two parts: feasibility (does it achieve reliable software?) and cost-effectiveness (is it cheaper than the traditional development process?). Although this project has delivered a working system, the objective was not to have a new system per se, but to better understand the development process. The reason an actual system was developed was to give confidence that the development process does work in reality. It is also expected that this will help the NSA's desire to disseminate the results of this project widely through conferences, journals, and their own internal government communications media.

Additional information about the Tokeneer ID Station can be found in the *EAL5 Demonstrator: Summary Report* and the *Overview and Reader's Guide* documents included in the case study materials.

Student Instructions

None at this time.

Instructor notes

While we have not developed case studies for this project, elements of it can certainly be used in lecture materials and classroom examples. Student analysis exercises and longer student projects can be developed from these materials. Rod Chapman specifically suggests the following as sources of classroom examples and case studies:

1. The formal security policy specification.
2. The formal functional specification - an example of a non-trivial Z specification with security properties etc. etc.
3. The code - an example of static verification and theorem proving.

Example solution

None at this time.

References

Barnes, J., Chapman, R., Johnson, R., Widmaier, J., Everett, B., Cooper, D. 2006. “Engineering the Tokeneer Enclave Protection Software”, Proceedings of the 1st IEEE International Symposium on Secure Software Engineering (ISSSE). Washington, D.C.

Chapman, R. 2011. “Tokeneer ID Station: Overview and Reader’s Guide”, S.P1229.81.8, Issue: 1.7, Altran Praxis Limited: Bath, UK.

Cooper, D., Barnes, J. 2021. “Tokeneer ID Station: EAL5 Demonstrator Summary Report”. S.P1229.81.1, Issue: 2.0, Praxis High Integrity Systems Limited: Bath, UK.

J. Woodcock, E. Gökce Aydal, R. Chapman “The Tokeneer Experiments” in Reflections on the Work on C. A. R. Hoare. C. B. Jones et al. (Eds), Springer Verlag 2010. pp. 405–430. ISBN 978-1-84882-911-4