Cyber-Resilient Architectural Patterns

Submitted by Anonymous on Mon, 05/06/2019 - 3:24pm. Contributor: Darren Cofer
Cyber vulnerabilities are often discovered during penetration testing of new systems. Even worse, they may be discovered after a system has been fielded, necessitating extremely expensive and time-consuming remediation. This is not a sustainable development model. Experience shows that this approach is both ineffective (due to the incomplete nature of testing) and results in long and expensive rework cycles. What is needed instead is a new engineering environment that allows systems engineers to design-in cyber-resiliency throughout the development process, enabling appropriate trade-offs among competing system requirements. Today’s systems engineers are given no development tools to help answer even basic cyber-related questions: "Is my system vulnerable to cyber exploit? And if so, how do I take action to make my system cyber resilient?"

As part of DARPA’s Cyber Assured Systems Engineering (CASE) program, we are developing advanced formal methods modeling and analysis tools to create an engineering environment for building cyber resilient systems. Our prototype tools provide verification of cyber requirements via a formal model of the system architecture with integrated model checking and information flow analysis. We track the satisfaction of cyber requirements throughout the design process by creating an assurance case that is integrated with the system architecture model. We help developers to address cyber requirements through a library of cyber-resilient design patterns, implemented via tool-assisted model transformations utilizing verified cyber-resilient components. Cyber-resilient implementations are automatically generated from the verified design model using property-preserving transformations, verified components, and the formally verified seL4 microkernel.

During their development, the tools are being applied to example design challenges based on the Unmanned Systems Autonomy Services (UxAS) framework developed by researchers at AFRL. In later phases, we will demonstrate effectiveness of the approach by applying our tools to challenge problems for the mission computing system in a military helicopter.

**Darren Cofer** is a Fellow in the Trusted Systems group at Collins Aerospace. He earned his PhD in Electrical and Computer Engineering from The University of Texas at Austin.

His principal area of expertise is developing and applying advanced analysis methods and tools for verification and certification of high-integrity systems. His background includes work with formal methods for system and software analysis, the design of real-time embedded systems for safety-critical applications, and the development of nuclear propulsion systems in the U.S. Navy.

He has served as principal investigator on government-sponsored research programs with NASA, NSA, AFRL, and DARPA, developing and using formal methods for verification of safety and security properties. He is currently the principal investigator for Collins teams working on DARPA’s Cyber Assured Systems Engineering (CASE) and Assured Autonomy programs.

Dr. Cofer served on RTCA committee SC-205 developing new certification guidance for airborne software (DO-178C) and was one of the developers of the Formal Methods Supplement (DO-333). He is a member of the RTCA Forum for Aeronautical Software, the Aerospace Control and Guidance Systems Committee (ACGSC), and a senior member of the IEEE.

**License:** Creative Commons 2.5