USAF Scientific Advisory Board Study

Cyber Vulnerabilities of Embedded Systems on Air and Space Systems

Study Abstract

The USAF Scientific Advisory Board (SAB) study on Cyber Vulnerabilities of Embedded Systems on Air and Space Systems was tasked to survey the use of embedded systems and assess potential cyber vulnerabilities and specific attack vectors that could affect each major category of embedded systems. The SAB considered the difficulties to an adversary in implementing such attacks as well as identifying how such attacks might be detected and the likely resulting mission impacts. The Board was also tasked to specify any immediate steps that should be taken to reduce cyber vulnerabilities in existing air and space systems, and to generate a roadmap for technology development that will result in less-vulnerable embedded systems in the near-, mid-, and far-term.

The Study Panel gathered extensive data from a wide cross-section of academia, commercial, and cyber defense designers, manufacturers, operators and users to assess the state of both capabilities and vulnerabilities of embedded systems. The foundation for the SAB's recommendations was four fold. First, embedded systems face distinct challenges separate from networked IT and commercial embedded systems (e.g., auto, aircraft, industrial control) but can leverage their lessons learned. Second, conventional protective strategies are insufficient to mitigate current cyber vulnerabilities. Third, the Air Force does not currently have sufficient embedded system expertise to provide long-term vulnerability mitigation across the acquisition lifecycle against an adaptive threat. Fourth, while the Panel concluded there is no silver-bullet solution, there is a broad-based set of immediate actions that can significantly mitigate embedded system cyber risk above and beyond basic hygiene.

The rigorous analytical framework by which the SAB approached this tasking led to several recommendations to mitigate cyber vulnerability of USAF embedded systems. The USAF should:

1. Ensure software integrity: Employ digital signatures/code signing. Require future systems to cryptographically verify all software/firmware as it is loaded onto embedded devices.
2. Mandate inclusion of software assurance tools/processes and independent verification and validation using appropriate standards as part of future contracts for all USAF systems. Use best commercial code tools and languages.
3. Employ hardware/software isolation and randomization to reduce embedded cyber risk and improve software agility even for highly-integrated systems.
4. Improve and build USAF cyber skills and capabilities for embedded systems.
5. Adapt Air Force Life Cycle Management Center cyber-resiliency requirements process to embedded systems.
6. Protect design/development information. Implement security procedures sufficiently early that protection against exfiltration and exploitation is consistent with the eventual criticality of the fielded system.
7. Develop situational awareness hardware and analysis tools to establish baseline embedded operational patterns and inform best mitigation strategies.
8. Develop and deploy continuously verifiable software techniques (e.g., dynamic attestation).
9. Develop and deploy formal-method software assurance tools and processes specific to USAF embedded systems.
10. The Air Force should work with defense microelectronics agencies to deploy trusted methods compatible with off-shore manufacturing.

Department of the Air Force SAF/PA Cleared this Information Jul 6, 2015 for Public Release
PAIRS Case Number 2015-0327