Tutorial Title: Securing your Embedded Systems for Cyberspace

Authors: Michael Vai, Roger Khazan, Ben Nahill

Are you an embedded system designer looking to enhance your understanding of cyber-security challenges and design principles? This system-architecture-level tutorial is designed to provide a balance of breadth and depth to help make your system secure from the start.

The tutorial will start by reviewing example embedded applications to establish security goals and potential threat models. We will then introduce an extensive overview of security technologies to achieve goals of confidentiality, integrity, and availability given design criteria and a realistic threat model. The technologies range from practical cryptography and key management, protection of data at rest, data in transit, and data in use, and tamper resistance. The tutorial concludes with an example secure embedded system designed with the introduced technologies.

This tutorial is designed for embedded system designers, hardware and software engineers, and program managers interested in an overview and introduction to cyber security with emphasis on embedded computing.

The tutorial draws from the authors' decades of combined experience in secure, resilient systems and technology.

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.