Featuring

Machine Vision

Protecting Machine Learning Algorithms with the EmSPARK™ Security Suite

INTRODUCTION

Machine Vision (MV) technology provides inspection and analysis using imaging. It is used in applications including industrial automation, process control, robotics, vehicle guidance, and logistics. An industry-leading vendor of machine vision products required a solution to protect its Artificial Intelligence and Machine Vision (AI/ML) algorithms used to support its technology.

THE PROBLEM—PROTECTING BUSINESS-CRITICAL INTELLECTUAL PROPERTY BY SECURING AI/ML APPLICATIONS

Machine Vision products follow the process of 1) acquiring an image of a product or process, 2) processing the data delivered by the image, and 3) making critical decisions (such as quality or acceptance of a product or process) based on the data. The algorithms that deliver this functionality represent critical intellectual property (IP), and create significant value for the products. It is absolutely business critical that these algorithms are protected, and can only be seen and used by developers of the products themselves. When designing, manufacturing, and provisioning MV products, application protection must be provided.

THE EmSPARK™ SOLUTION

The industry-leading Machine Vision vendor selected Sequitur's EmSPARK™ Security Suite in order to protect its critical IP, which would be required during product design, manufacturing, and deployment in the field. The following EmSPARK™ features and functions were implemented:

- EmSPARK™'s CoreTEE™ operating system creates a secure enclave, separating secure applications and data from traditional "rich" applications (such as Linux and OpenSSL).
- EmSPARK™ provides trusted applications (TAs) for key and certificate management, secure storage, and cryptography to ensure protection of critical data. An end-to-end secure boot, update and failure recovery process was implemented to protect the product's firmware integrity in manufacturing and deployment.

- Using EmSPARK™'s Software Developer's Kit (SDK), the vendor was able to develop applications that would house their algorithms in the CoreTEE's Secure Enclave.
- EmSPARK™ APIs enabled secure communication between the secure applications and the rich applications during device operation.
- By providing encrypted code, housed in the EmSPARK™ secure environment, the vendor was able to ensure that the algorithms would be protected during the manufacturing, software provisioning, field deployment, and firmware upgrade stages of the Machine Vision product's life cycle.

Learn More

EVAL KIT Get Started with Free Evaluation Kit: EmSpark™ Security Suite

Download: EmSPARK™ Whitepaper

A **FREE** Evaluation Kit for the EmSPARK™ Security Suite is available at: https://www.sequiturlabs.com/emspark/free-eval-kit/.

SEQUITUR LABS

Sequitur Labs is developing seminal technologies to improve trust in a connected world, reducing the cost and complexity to build secure embedded and IoT devices. Sequitur's products span a range of disciplines required for trusted computing, from boot through the full device lifecycle. Sequitur's security solutions provide real business value to device makers, such as reducing BoM costs, protecting revenue by thwarting IP theft, improving product reliability and reducing liability, and improving device lifecycle management processes. To learn more about Sequitur's security platform, visit us at www.sequiturlabs.com.

PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

Photos provided by Arseny Togulev & Mika Baumeister on Unsplash.
MCSEm-0003-RevC. Printed in the U.S.A.