NUVATION ENGINEERING

WHITEPAPER

Important Design Considerations for Electronic Devices

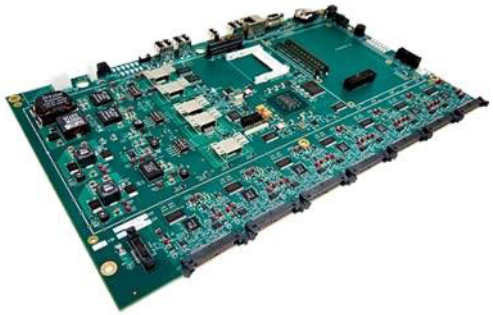
Part 4: Data Security

AUTHOR: ALEX LEBLANC
LEAD HARDWARE/SOFTWARE DESIGNER

Over the past two decades Nuvation Engineering has developed data acquisition systems for a wide range devices and market applications. Based on our experience performing hundreds of engineering design projects, our engineers have identified several key considerations that require special attention during the planning, design, and development of data acquisition systems.

> *"Security is always excessive until it's not enough."*
> — Robbie Sinclair, Head of Security, NSW

We live in an increasingly data-driven world. It's not uncommon to have dozens of devices on a home wireless network - smart televisions, scales, treadmills, doorbells, lightbulbs, receptacles, switches, thermostats, refrigerators, and even toasters. It's making our lives easier and we love having the latest-and-greatest gadgets. As science fiction becomes science fact, we're all eagerly waiting for replicators and teleportation devices.



Nuvation worked with a client in the life sciences industry to develop a data acquisition system for a flow cytometer device.

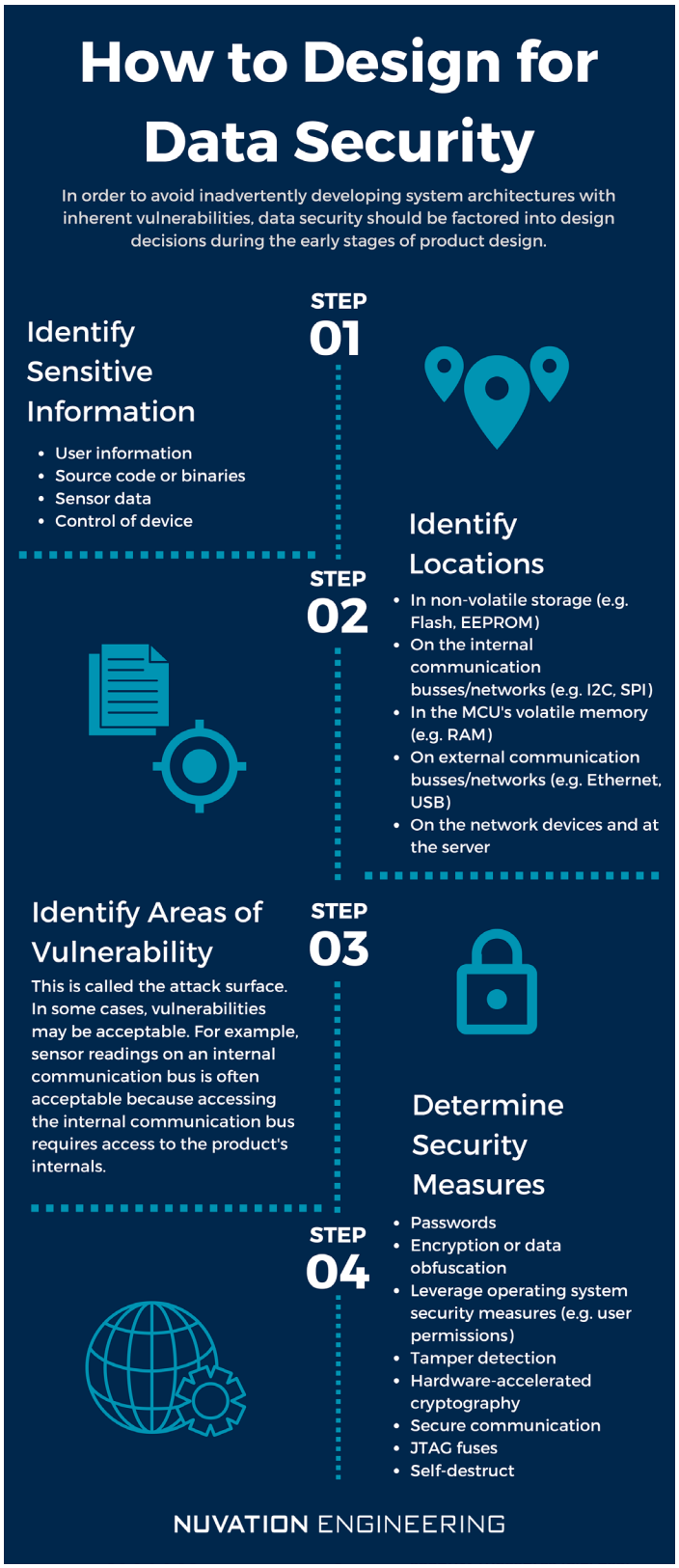
With ever-increasing data comes an ever-increasing need for data security. Bad actors - cybersecurity adversaries trying to get to your data - are getting better and are keeping up with data security advancements.

Data security refers to the protection of data against unauthorized access. This data can be sensor data, algorithms, source code, files, logs, user data, or any other type of information. Different types of data have different intended audiences. For example, source code and algorithms are typically not intended to be accessible by the user. In order to prevent unauthorized access to sensitive data, data security can be implemented.

Vulnerabilities and How To Improve Security

In order to avoid inadvertently developing system architectures with inherent vulnerabilities, data security should be factored into design decisions during the early stages of product design. Late-stage modifications to system architecture can be incredibly costly and can impact the schedule. Many small companies have been bankrupted by a product recall due to critical security flaws in the design; data security cannot be an afterthought!

Data security requirements have important impacts on the underlying hardware platform. For example, can the data encryption (or obfuscation) be handled by an MCU with the right combination of hardware blocks? Alternately, the complexities of high-speed data acquisition and control might make a specially designed FPGA a better solution.



The *first step* is to identify the sensitive information. For example:

- User information
- Source code or binaries
- Sensor data
- Control of device

The *second step* is to identify all the locations where the information will be present. For example:

- In non-volatile storage (e.g. Flash, EEPROM)
- On the internal communication busses/ networks (e.g. I2C, SPI)
- In the MCU's volatile memory (e.g. RAM)
- On external communication busses/ networks (e.g. Ethernet, USB)
- On the network devices and at the server

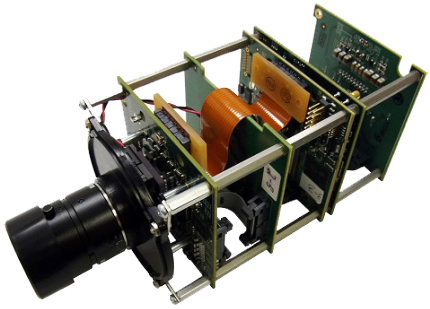
The *third step* is to identify in which of these areas exist vulnerabilities that need to be addressed. This is called the attack surface. In some cases, vulnerabilities may be acceptable. For example, sensor readings on an internal communication bus is often acceptable because accessing the internal communication bus requires access to the product's internals.

The *fourth step* is to determine the appropriate data security measures that can put in place. These measures should be included in the Product Requirements Document (PRD). For example:

- Passwords
- Encryption or data obfuscation
- Leverage operating system security measures (e.g. user permissions)
- Tamper detection
- Hardware-accelerated cryptography
- Secure communication
- JTAG fuses
- Self-destruct

Defining these requirements early enables the design engineers to develop a system architecture that is compatible with the requirements. For example, a device performing high-speed data acquisition of sensitive data is likely to require hardware encryption, which may require specialized circuits or an FPGA.

Nuvation designed an Image Media Block for a Digital Cinema Projector, which included the hardware to ingest, decode, watermark, and play cinema video, all within a high-security boundary. For the video and audio processing, Xilinx Virtex-6 and Spartan-6 FPGAs were used.



Nuvation designed a 3-D camera system for use in military vehicles on the battlefield.

For FIPS 140-2 Level 3 (security standard for cryptographic modules) compliance, FPGA-based security monitoring was implemented. Critical security parameters (CSPs) were cleared when tamper-detection/response circuitry detected that the enclosure was being tampered with (e.g. covers/doors are being opened).

Nuvation designed a Data Acquisition System for a Flow Cytometry (FCM) Device, a medical product which was designed to perform 14-bit, 25 MSPS analog data acquisition on 14 channels and featured a Xilinx Kintex-7 FPGA.

Nuvation has also designed a high-speed high definition CCD Camera, which used an Altera Cyclone IV FPGA for a customer in the defense industry.

The Importance of Data Security

Data security protects your intellectual property (IP). Without proper data security measures in place, your algorithms and source code are vulnerable to reverse engineering by competitors. Accessible software binaries can be disassembled.

Security features may be a major selling point that can differentiate a product from its competitors. In some cases, a company may even be held liable by consumers and governments as a result of personal data breaches.

A malicious user who finds a vulnerability and is able to perform arbitrary code execution (ACE) has the ability to reverse engineer the product, falsify warranty claims, enable locked features, compromise a user's private data, destroy information, and even use the product for criminal activity.

A user's personal data can be used for identity theft, blackmail, scams, and undesired targeted advertising. Nuvation designed a device for Identify Verification for Payment Processing. This

device featured a technologically advanced and safe way to make payments using fingerprints as identification and payment configuration. The data security for the user's personal information and payment information is a critical feature of this product.

Even seemingly harmless data, such as heart rate logs from a smartwatch, could be used by companies to discriminate based on medical history. Nuvation has designed a number of medical products that captured sensitive medical information, such as a Remote Health Care Monitoring device that communicates with a central database over a wireless network. It is critical that patient medical information remains secure.

Nuvation developed a remote health care monitoring device.

In the past few years, there have been numerous news reports of hackers getting access to unsuspecting families' baby monitors and security cameras due to their poor data security measures. Smart home device data (such as smart thermostats, smart locks, home assistants, and doorbells) can be accessed by criminals to determine when a home is unoccupied.

Nuvation designed a Home Monitoring Sensor for temperature and occupancy detection. Since this sensor's data could expose information on a home's occupancy, we implemented custom radio protocols for the SRD radio band to improve security and prevent unauthorized access.

Nuvation also designed a Stereoscopic Retail Analytics Camera that tracks shopper behavior within a retail store, to help marketers make merchandising decisions. An unauthorized user could get information on occupancy and even disable the camera before a store robbery. For this reason, it is important that proper data security measures be in place to prevent unauthorized usage of the camera.

Contact us to learn how we can provide system security services for your product design.

FOR INQUIRIES, PLEASE CONTACT:

NUVATION ENGINEERING

T: (888) 669-0828

E: info@nuvation.com