Security from Inception Suite
Unique set of tools and services for the development and provisioning of embedded applications

Start your security journey.
Security from Inception

Security is a journey, rather than a destination, and it is true that no system will ever be completely protected. The rapidly growing market of connected devices is facing major security challenges, with attacks ranging across IP theft, counterfeiting and overproduction, as well as data theft and potentially life-threatening sabotage. In order to solve these security challenges in a scalable and sustainable way, application security must be implemented right from start of the development cycle, to achieve security from inception.

Security from Inception is built upon the establishment of a robust, yet flexible, Root of Trust, leveraging the security functionality of secure devices, or providing a sustainable foundation for existing devices and applications. Vulnerabilities are minimized, updates and patches are authenticated and individualized, and lifecycles are managed protecting your application today and into the future. Threats will not stop - so Secure Thingz and IAR Systems are working with industry leaders to make superior security available for all – delivering a secure and sustainable future for connected devices.

Our Security From Inception Suite enables your organization to build a platform which will extend with evolving security needs as threats appear, and as legislation impacts your business. The Security from Inception Suite provides companies with a straightforward way of building the right level of security for their application needs throughout the development, manufacturing, and product management process.

In addition, Secure Thingz is working closely with industry-leading providers of secure elements, microcontrollers, and microprocessors to deliver secure devices for the IoT.

Security is the top concern for companies worldwide

Less than 4 percent of new IoT devices have embedded security today.

By 2035, there will be a trillion connected devices.

Counterfeiting costs companies approximately $500 billion annually.

55 percent of organizations have had to manage the public scrutiny of a breach.
Evolving legislation for IoT security

IoT security requirements are evolving rapidly, with guidelines now present in many global markets. As an example, from January 1, 2020, it is a legal requirement that all connected devices sold in certain US states must meet fundamental capabilities including enhanced password mechanisms, vulnerability disclosure, patching and update mechanisms, plus the ability to formally authenticate the device. The Security from Inception Suite has been designed to enable developers to rapidly meet these emerging requirements.

These are some of the most recent legislation evolvements around the world:

Europe
- GDPR – In effect with fines of €20M or 4% global revenue
- UK Government – Published 13 Codes of Practice. Legislated enforcement within 3 years with GDPR-type fines
- ETSI – Reiterating UK guidelines
- EU (ENISA) – >150 baseline recommendations

North America
- California - IoT security law effective from January 1, 2020
- USA - NIST evolving cybersecurity act

Asia
- Korea – The Ministry of Science and ICT and the Internet & Security Agency certification
- China – Official standards released by government-sponsored working group

Best practices for IoT devices

For consumer electronics, the IoT Security Foundation, in alignment with regulatory bodies around the globe including the EU, US, UK, Japan, Singapore, South Korea and others, have published best practice guidelines requiring the following security measures:

1. Monitor System telemetry data
2. Simplify customers ability to delete personal data
3. Implement a Vulnerability Disclosure Policy
4. Make installation and management easier
5. Securely store credentials & security sensitive data
6. Validate input data
7. No default passwords
8. Make systems resilient to outages
9. Ensure personal data is protected
10. Ensure Software integrity
11. Minimise exposed attack surfaces
12. Communicate securely
13. Keep software updated

Securing the supply chain

The OECD (Organization for Economic Cooperation & Development) has estimated that the global trade in counterfeit goods exceeds $500 Billion annually. Whilst this encompasses many different types of goods, the electronic systems component is probably the largest by value. From chips to automotive sub-assemblies, and from industrial motors to medical infusion pumps, companies are continuing to lose profits to counterfeit products.

Securing the supply chain is a critical component of the security story and in many ways more important than a theoretical hack. It impacts the profitability of companies, it enables competition from 2nd and 3rd tier vendors, and it steals from the research dollars the market leaders spend to evolve the market.
Developing with security

The complete development toolchain IAR Embedded Workbench provides developers with everything they need in their development workflow. C-Trust works as an extension to IAR Embedded Workbench and enables developers to easily protect an existing or new application. Embedded Trust and C-Trust deliver an unrivalled security development environment for embedded systems. These tools enable organizations to use pre-defined Security Context Profiles, ensuring that they remain in control of system operation today, and into the future.

Security Context Profiles define the configuration of the trusted execution environment. It is a description of the security environment that is required to protect your application. With C-Trust, developers are able to rapidly apply Security Context Profiles to application development, ensuring consistency and reducing development effort. With Embedded Trust, organizations are able to define custom Security Context Profiles, which uniquely service their specific needs. Security Context Profiles enable organizations to simplify:

- Complex cryptographic device identities and ownership structures
- Creation of a robust Root of Trust, ensuring device authentication, authorization and attestation, the core proofs of identity
- Implementation of security hygiene, dependant on device hardware support
- Secure Boot Manager extensions to support core boot functionality
- Application of patches, updates, and other lifecycle management criteria
- Delegation of identity for onboarding into cloud infrastructure applications

These Security Context Profiles provide the foundation for a set of core security concepts, enabling Security from Inception, including protection of Intellectual Property, which is about inhibiting IP theft and malware injection, and production control, which is about protecting keys across development and production.

The Secure Boot Manager, delivered as a component of Embedded Trust and C-Trust, is the first software component to gain Security Evaluation Standard for IoT Platforms (SESIP) certification, ensuring that everyone can build on secure foundations.
Secure provisioning

Security-orientated development is traditionally challenging as there is a need to manage high-value code and secrets, including keys, along the complete supply chain from development through to production, often at remote sites or delegated to contractors.

The Security from Inception Suite enables developers to make the first critical step by building security into their designs ready for production. Secure Desktop Provisioner has now been added as a critical component of the Security from Inception Suite. For the first time, it is possible to take the second step of securely transferring those designs to a production environment to produce prototypes and first articles that fully implement the designed security features. In Embedded Trust and C-Trust, development keys are replaced by secure production keys, during the creation of a final, secure production package. The Secure Desktop Provisioner imports these production packages.

**Secure Desktop Provisioner** enables developers, who have defined their key infrastructure during development, to dynamically generate keys and "provision" these securely into the device together with programming a cryptographically secured image of the application.

Provisioning is the act of injecting unique characteristics to every device being produced, whether at the chip, board or system level. This unique cryptographic identity, similar to a birth certificate, enables every programmed device to be identified and acted upon, whether this is to provide authentication, or to enable updates to be targeted to a single device, or a group. The provisioning is often implemented alongside secure programming, ensuring as much information is protected as possible.

Training services enabling Security from Inception

The Security From Inception Suite includes a wide array of training resources suitable for developers, management and corporate leadership looking to understand how security will impact their businesses. It is structured in different set of training, enabling developers to gain a clear overview of demands, but also ensuring that other stakeholders, such as the Corporate Information and Security (CISO) functions, can align with product security demands.

<table>
<thead>
<tr>
<th>Available training</th>
<th>BASIC EDITION</th>
<th>ADVANCED EDITION</th>
<th>PREMIERE EDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Embedded Security – 2 days</strong>&lt;br&gt;<strong>Suitable for organizations who are new to security</strong></td>
<td>2 seats at scheduled training</td>
<td>2 seats at scheduled training</td>
<td>Up to 8 seats, on-site training</td>
</tr>
<tr>
<td>Topics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Developing IoT Applications with Embedded Trust &amp; C-Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Impact of legislation &amp; security on IoT applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Managing Intellectual Property &amp; Inhibiting Overproduction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Embedded Security – 1 day</strong>&lt;br&gt;<strong>Suitable for organizations who want to get a deeper understanding of security</strong></td>
<td>2 seats at scheduled training</td>
<td></td>
<td>Up to 8 seats, on-site training</td>
</tr>
<tr>
<td>Topics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Introduction to IoT Cryptography &amp; Security Practices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Implementing the 13 Best Security Practices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Premiere Training or Design review – 1 day</strong>&lt;br&gt;<strong>Suitable for organizations who want to dig deep into different security mechanisms and/or want a custom design review</strong></td>
<td></td>
<td></td>
<td>Up to 8 seats, on-site training and review</td>
</tr>
<tr>
<td>Choose 2 of the following topics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Embedded Security - Device Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Embedded Security - PKI Techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Custom Design Review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Our Design Review team will work with your development staff to help define the protection profile your system requires, and how to optimally implement security to meet your commercial goals.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Training topics

Basic

Developing IoT Applications with Embedded Trust & C-Trust
This training introduces the basics of developing embedded applications with security. Reviewing the concepts of identity, the development of a Root of Trust, and the overarching Security Context Profile, the training examines the practical implementation of security using Embedded Trust, and IAR Embedded Workbench with C-Trust.

Impact of Legislation & Security on IoT Applications
Legislation surrounding connected devices is already present, with governments across the US, EU and Asia Pacific rapidly implementing guidance and best practice. As a founding member of the IoT Security Foundation, a primary contributor to the legislation, this training will examine what is expected and how developers can build resilient systems for today and for the future.

Managing Intellectual Property & Inhibiting Overproduction
The OECD estimates that cloning, counterfeiting and overproduction of goods is a $500 Billion per year industry. The impact on companies of having critical IP stolen, and of having counterfeit goods in their supply chain is massive. Properly implemented security can inhibit all of these challenges, protecting valuable software R&D, and ensuring that services revenues are guarded. This module highlights how security encrypts and manages software through the development and production cycles.

Introduction to IoT Cryptography & Security Practices
This training focuses on the implementation of specific cryptographic requirements for IoT devices, including aspects of symmetric and asymmetric cryptography, key management, certificate structures and basic Public Key Infrastructure. It is ideal for those focusing on the implementation of security into devices, understanding the evolution of security into advanced products with lifecycle management demands.

Implementing the 13 Best Security Practices
The 13 Best Security Practices have been evolved to give clear guidance on the fundamental security requirements for consumer connected devices. These best practices form the framework for the majority of the legislation globally. In this training, we will review how these Best Practices can be applied within IoT device security to provide a robust and sustainable platform for future proof devices.

Premiere

Embedded Security - Device Authentication
Device authentication is a baseline requirement for all legislative requirements in the IoT domain. However, authentication has many other uses, including how we pair devices from vendors (e.g. power tool and battery pack, or printer and cartridge), and how we closely pair high-value services with specific devices. Device authentication is a broad domain, and this training introduces many of the different use cases and implementation techniques.

Embedded Security - Secure Cloud Onboarding
Connecting devices to cloud services is a rapidly growing requirement. However, the onboarding process is often challenging with multiple stakeholders having to exchange trust as part of formal onboarding process. This training reviews the core requirements for Secure Cloud Onboarding and examines a number of example implementations.

Embedded Security - PKI Techniques
This training is focused on enabling engineers to understand more technical details of Public Key Infrastructure (PKI), and the implementation required for future generation of device authorization and authentication. While many systems can be built today with standard or simple key exchanges, the requirements for a fully operational IoT will require more flexible and robust systems based on PKI techniques.

Custom Design Review
Our Custom Design Review supports a review of the organization’s security requirements and implementation. Starting with a review of the potential risks and threat model, including what requires protect, and from whom, the review then will support the creation of custom Security Context Profiles to best meet the market need.
The Security from Inception Suite is created by Secure Thingz and IAR Systems.

Secure Thingz is the global domain expert in device security, embedded systems, and lifecycle management. Since 2018, the company is part of IAR Systems, the future-proof supplier of software tools for embedded development.

Secure Thingz is focused on delivering advanced security solutions into the emerging industrial Internet of Things market, alongside critical infrastructure, automotive and other markets. The company is a founding member and Executive Steering Board member of the IoT Security Foundation, the leading global organization for IoT Security.

Start your security journey today!
Contact us to get started.

www.iar.com/securityfrominception