timesys®

Secure by Design: Timesys TRST Security Services

Implementing security early in the design of your device is key to managing its security

When it comes to IoT systems with open source components, ensuring your devices have the proper security posture means planning ahead. But time-to-market pressure can lead to sacrificing security planning at the design stage.

Now you can address security early in the design of your products and bring products to market faster, and more secure. Timesys TRST Security Services enable you to implement security best practices including secure boot, encrypting data, authenticating users and servers, over-the-air (OTA) updates, and use trusted execution environments to keep confidential data and algorithms private.

Timesys TRST "Secure by Design" services enable you to bring products using embedded Linux and Open Source Software to market faster, without compromising security.

No matter what stage your embedded product development is in, you can rely on Timesys TRST Security Services to help you:

- **Reduce the attack surface of your device** — By auditing, hardening, optimizing your software footprint, and implementing secure boot and chain of trust, we improve the security posture of your device.
- **Reduce performance trade-offs** — By selecting the proper hardware, you can minimize the performance impact of securing it. Timesys has the expertise to help you achieve the lean footprint and lower power consumption you need, even while meeting security requirements.
- **Reduce time-to-market delays** — Through our Security Services, security is baked in at the outset of your development, enabling you to cut the time, rework, and cost overruns that often come with deploying security too late in design.

TRST Timesys to help you with your product security

When you engage with Timesys, you can rely on our expertise to implement security into your product design. We've worked with hundreds of boards, on thousands of projects and with numerous build systems including: Yocto Project, Timesys Factory, Buildroot, PetaLinux, and LTIB. Our years of experience have enabled us to provide you with a solution that delivers security best practices in the most cost-efficient way possible.

"Security is critical for today's IoT and embedded systems. Medical devices, retail point of sale, and industrial control systems handle sensitive data, so the security of devices used in these applications is essential. We're partnering with Timesys to highlight best practices for designing and maintaining security in systems using our feature-rich and performance-scalable i.MX applications processors."

– Robert Thompson, i.MX Ecosystem Manager at NXP

Timesys TRST Security Services

To help you secure by design, Timesys offers TRST Security Services in a variety of areas.

Secure by Design: Implement Device Security During Development

Secure Boot/Chain of Trust

Ensure your device is not running tampered software by verifying its authenticity before execution. Establish software authenticity all the way from the bootloader to user applications. Our secure boot services help implement:

- Verified bootloader (NXP i.MX / QorIQ, Qualcomm Snapdragon, TI Sitara, Atmel SAMA5, Xilinx Zynq, Intel® x86 and Atom™, and more)
- Kernel verification (FIT image, SoC specific mechanisms)
- Root filesystem verification (dm-verity, IMA/EVM, FIT image)

Device Encryption and Secure Key Storage

You can protect IP and sensitive user information by encrypting data/software. It is also critical to protect the key used for encryption using a secure storage mechanism. Additionally, software that handles confidential data should run from within a hardware/software-isolated environment.

We provide solutions and services that span:

- Anti-cloning (IP and Data Protection)
- Key Management and secure key storage
- Data protection using encryption — In use, in motion, and at rest
- Trusted Platform Module (TPM)
- Trusted Execution Environment (TEE) using Arm TrustZone and OP-TEE
- Device identity and authentication

OTA Software Updates

Our security services can help you determine how to update/deploy software securely and deny unauthorized software installs.

- Over-the-air (OTA) updates of the software on your embedded system
- Package updates
- Full OS updates
- Signing of packages and images
- Server authentication

Security Audit

By performing a risk analysis, our audit services can help you determine what potential threats your system might encounter and what should be secured. Timesys' security audits:

- Provide a detailed review of packages and default system configuration
- Run & analyze reports from audit and scanning tools
- Provide you with an end-to end-review of system security
- Provide you with a risk management and recovery plan

Hardening

Our hardening service focuses on system configurations needed to reduce your product's attack surface, decrease risk of compromise, and minimize breach impacts including:.

- Access & authorization
- Vulnerability
- Logging of all user access
- Logging of access level changes by any program
- Disabling unused services and ports
- Security-oriented configurations for packages and kernel

To learn more about Timesys TRST Security Services for devices based on embedded OSS, email us at **sales@timesys.com** or call us at **1.866.392.4897** (toll-free) or **+1.412.232.3250** to schedule a complimentary, no-obligation consultation.

Disclaimer: *Security is an ongoing process and is not foolproof. Timesys' security offering provides assistance with minimizing known vulnerabilities based on known issues, but doesn't have any warranty.*

timesys®

Headquarters / North America Office:
1905 Boulevard of the Allies,
Pittsburgh, PA 15219 UNITED STATES
1.866.392.4897
sales@timesys.com

EMEA Office:
ul. Palmowa 1A,
62-081 Chyby POLAND
+48.53.733.8080
emea@timesys.com

APAC Office:
3rd Floor, Jaag Homes, Achyutha Square,
No. 3, MTH Road, Villivakkam,
Chennai, Tamil Nadu – 600 049 INDIA
+91.0124.4299897
apac@timesys.com