SEC-Line ELEMENTS

Security building blocs for Embedded Computers

- APPROTECT: hardware enforced application integrity and confidentiality.
- TRUSTED BOOT: measure system software with TPM secure element
- AUTHENTICATION: TPM based authentication for SSL/TLS secure communication
- SECURE BOOT: boot only signed software from the BIOS firmware
- VULNERABILITY WATCH: Subscribe to information regarding software vulnerabilities

POSSIBILITIES START HERE kontron S&T Group

SECURITY CHALLENGES IN EMBEDDED COMPUTING

Digital security is of tremendous importance for embedded computing: the exploding number of deployed autonomous devices with no operator close by will represent a significant surface of attack. Moreover, embedded computers can be connected and active in the field during many years.

The main threats are linked to confidentiality, integrity and availability. It is critical that no one can look at the data which are secret or represent an asset for the owner. But integrity is also of utmost importance since it would be a disaster if compromised data would be silently injected into the application.

Kontron answers digital security requirements with SEC-Line platform, a turn-key solution hardened with hardware enforced root of trust (secure elements), and software only techniques such as Secure Boot available in server router products.

For customers integrating their own secure platform, Kontron also provides the key building blocs used in SEC-Line platforms individually.

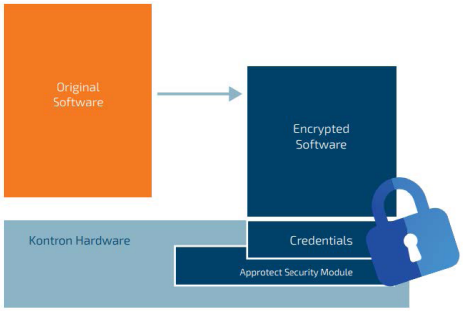
With this approach, customers build their secure solutions by mixing Kontron hardware root of trust with their own security ingredients.

APPROTECT: PROTECTION OF THE APPLICATION CODE

APPROTECT addresses the main security threats for applications deployed within computers:

- **Garanteed Integrity:** the running application cannot be hacked. Patching the binary, either on the disk or in memory, to work around license checks is impossible.
- **Absolute Confidentiality:** the cleartext of the application code is not available to prying eyes, forbidding any attempt to reverse engineer it in order to learn or to reproduce its behavior.
- **Copy Protection:** the embedded systems (software application or full equipment) cannot be cloned and deploy multiple copies of the application without authorization.

The APPROTECT solution, using a security technology from an industry leader of IP protection, uses field proven encryption technology to protect the application thanks to the built-in security of a dedicated hardware secure element located on Kontron products. All or part of the application executable code is encrypted 'at rest' (on the storage device) and is only decrypted in memory when the associated keys stored inside the secure element are available. At run time, the integrity of the application in memory is also permanently checked. The application can be totally encrypted or some parts only (using a dedicated API). This approach allows to deploy full applications, and unlock features later, thanks to distinct license keys.



Software: Encryption of an application is performed by Kontron inside a dedicated security room by authorized personnel. Purchase of SEC-APPROTECT-INI allows for 10 encryptions service for the same project, allowing software updates this serviice includes the generation and delivery of the application key for one reference computer.

Hardware: each computer must have the application key loaded in its secure element to run the software. SEC-APPROTECT-T10 is used to procure keys for 10 more computers.

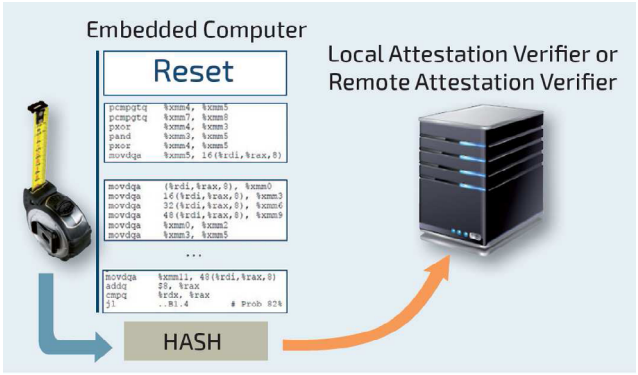
Note: In situations where a sensitive application cannot leave a company unencrypted, **On-Premises Encryption** is also possible with the use of a special encryption equipment. Contact Kontron.

TRUSTED BOOT TO DETECT SYSTEM SOFTWARE ALTERATION

Detecting any unexpected change of code, data or configuration during the boot process, starting from reset time, is a highly desirable feature to discover attempts to compromise the system.

The trusted boot mechanism relies on the TCG (Trusted Computing Group) international standard, where a Trusted Platform Module (TPM) secure element is used to verify the validity of the boot of a computer. The TPM measures through a hash value all pieces of code executed during the boot, including firmware, firmware setup, bootloader, operating system and more if needed. Any single bit change in the boot, as compared to a reference value, can be detected and reported in a local or remote cryptographic attestation, as illustrated below:

- **Trusted Boot**



This service exists for Kontron x86 computers equipped with TPM1.2 secure element and running Linux, with a target to support TPM2.0 soon.

SEC-TRUSTEDBOOT-INI contains:

- A new BIOS version for the target computer enabled with the trusted boot mechanism,
- TPM linux device driver code,
- Documentation to setup the computer (example),
- A Linux tool to compare, locally or remotely, the digest resulting of the boot to a reference value.

For the deployment phase, Kontron can duplicate the trusted boot setup of the reference machine to additional identical computers (boards + firmware + software) by ordering SEC-TRUSTED-BOOT-T10 items.

AUTHENTICATION WITH TPM TO SECURE NETWORK PROTOCOLS

To establish a secure network connection like https, a private key is needed on the server side at least, and also recommended on the client side for embedded computing since no operator is present to enter a password. It is often NOT a good idea to store the private key on the disk, even encrypted, because at some point, it will be decrypted in memory and CPU registers when used at the beginning of a network session.

With the TPM authentication, the private key will be stored and used under the hardware protection of the TPM, so that it is never exposed. Without this hardware protection, the risk exists of having the private key stolen, which would allow the duplication of a compromised server or client machine, or a man in the middle strategy spying the communication.

The TPM authentication service is available on Kontron x86 CPU boards and currently restricted to TPM1.2 version under Linux, with a target to support TPM2.0 soon. When ordering SEC-AUTHENTICATION-INI, the following items will be delivered:

- Configuration of the computer board + OS storage to perform TPM authentication.
- One SSL certificate signed by Kontron as a private root authority, with expiration date set according to customer requirement. Cryptography algorithm used will be RSA2048 and SHA1 (SHA256 when TPM2.0 implementation available).
- Kontron private root authority public key.
- A guide and tool to install and configure TPM authentication.

To get other SSL/TLS certificates for identical type of hardware+-software, order SEC-AUTHENTICATION-C10. For Kontron to duplicate the TPM authentication configuration on other identical type of hardware+software, including new SSL/TLS certificates, order SEC-AUTHENTICATION-T10.

SECURE BOOT TO RESTRICT BOOT TO SIGNED IMAGES

As a first security measure, it is highly beneficial that an embedded computer be restricted to boot from the firmware only authentic code, typically from a disk or SSD. That is the purpose of the secure boot.

The secure boot mechanism is a purely software security strategy at the BIOS level to prevent booting of a binary which is not properly signed. With this security in place which is protected by the BIOS passsword, no one can boot a software which is not explicitly listed as authorized.

The list of allowed signatures is stored in the BIOS firmware as a set of certificates and can be updated from a BIOS configuration menu.

The list of keys needed to activate the secure boot is the following:

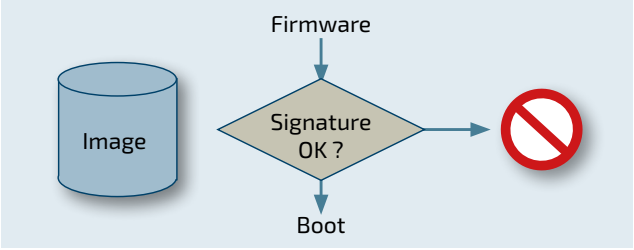
- PK Plateform Key: key of the hardware platform needed to verify the KEK keys.
- KEK Key Exchange Keys: key(s) of the owner(s) of the software to boot.
- DB key(s): key(s) of the different software image or version of software allowed to boot. Used to verify the signature(s) of the software to boot.
- DBX key(s): key(s) of software or version of software explicitely prohibited to be booted.

The secure boot service is available on Kontron x86 CPU boards running a UEFI BIOS firmware. Upon delivery of SEC-SECURE-BOOT-INI, the customer is getting the following items:

- A set of PK, KEK and DB certificates using a Kontron root signature. Includes the microsoft signatures allowing to boot Windows, Fedora and Ubuntu Linux.
- A guide to enter manually the certificates into the BIOS through the BIOS menus.
- A reference BIOS image containing the certificates.

In the case the set of secure boot keys has to be renewed, for example due to a software change or a BIOS change, SEC-Line-SECUREBOOT-K10 need to be ordered for new set of keys.

When it comes to deploying a frozen secure boot config-uration on numerous identical hardware+firmware, SEC-Line -SECURE-BOOT-T10 can be ordered at a quantity equal to the number of hardware to program.



SOFTWARE VULNERABILITY WATCH

Software vulnerabilities discovered during and after deployment may be a concern for embedded computers, as regularly demonstrated publicly in the news. With long life cycles and complex supply chains, embedded computers are especially exposed to malware attacks targeting older versions of OS distributions and silicon microcode.

Kontron Software Vulnerability Watch service allows customers to share the burden of monitoring published vulnerabilities, establishing the exposure level for already deployed equipment and providing the necessary fix.

SEC-Line SEC-Watch-SV is an affordable annual subscription for software vulnerabilities watch, on a program basis. It typically consists, for the Linux operating system environment, in defining the software bill of material, in monitoring the published vulnerabilities impacting the configuration, and when available from the software editor, in packaging and distributing the corresponding software fix.

ORDERING INFORMATION

ARTICLE	DESCRIPTION	
SEC-APPROTECT-INI	Per Application	Up to 10 application encryptions service over 2 years maximum. Also includes application key generation for one reference computer.
SEC-APPROTECT-T10	Per Application	Additional copies of application key for target boards / systems. Qty of 10 over 2 years maxi-mum.
SEC-TRUSTEDBOOT-INI	Per Project	Bios enabled for trusted boot, TPM linux driver and Linux tool to compare the hash of the boot to a reference value, locally or remotely.
SEC-TRUSTEDBOOT-T10	Per Project	Duplication of a reference trusted boot configuration on 10 more identical hardware+firmware+software configuration, over 2 years maximum.
SEC-AUTHENTICATION-INI	Per Configuration	Configuration and SSL/TLS certificate for a reference hardware+software configuration to perform authentication with TPM.
SEC-AUTHENTICATION-C10	Per Computer	Additional SSL/TLS certificates for 10 more identical hardware+software config, over 2 years maximum.
SEC-AUTHENTICATION-T10	Per Computer	Installation of a reference TPM authentication configuration, including SSL/TLS certificate, on 10 more identical hardware+software, over 2 years maximum.
SEC-SECUREBOOT-INI	Per Configuration	Configuration and certificates of secure boot for a reference hardware+firmware configuration.
SEC-SECUREBOOT-K10	Per Configuration Change	Renewal of up to 10 sets of the secure boot keys, due to new software or BIOS change, over 2 years maximum.
SEC-SECUREBOOT-T10	Per Computer	Duplication of a reference secure boot configuration on up to 10 more identical hardware, over 2 years maximum.
SEC-WATCH-SV	Per Configuration	Affordable annual subscription for software vulnerabilities watch, on a program basis. It typical-ly consists, for the Linux operating system environment, in defining the software bill of material, in monitoring the published vulnerabilities impacting the configuration, and when available from the software editor, in packaging and distributing the corresponding software fix.

ORDERING INFORMATION

SUPPORTED PLATFORMS	SEC APPROTECT	SEC-TRUSTEDBOOT	SEC-AUTHENTICATION	SEC-SECUREBOOT
SEC-APPROTECT-INI		yes	yes	yes
SEC-APPROTECT-T10		yes	yes	yes
SEC-TRUSTEDBOOT-INI		yes	yes	yes
SEC-TRUSTEDBOOT-T10		yes	yes	yes
SEC-AUTHENTICATION-INI	yes	yes	yes	yes
SEC-AUTHENTICATION-C10	yes			yes

GLOBAL HEADQUARTERS

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

www.kontron.com