SEC-Line

KONTRON SECURE EMBEDDED COMPUTING SEC-Line
Security for Embedded Computers

- APPROTECT: protect application integrity and confidentiality with hardware secure element
- TRUSTED BOOT: protect system software during boot with TPM secure element
- AUTHENTICATION WITH TPM: authenticate system hardware during SSL/TLS secure communication with TPM secure element
- SECURE BOOT: boot only signed software from the BIOS firmware
- SOFTWARE VULNERABILITY WATCH: be informed of software vulnerabilities affecting your configurations in the field and get fixes when available
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 hardware enforced root of trust (secure elements), and software only techniques such as Secure Boot.

Here is the Kontron SEC-Line computer security offering:

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROTECT</td>
<td>Application integrity, confidentiality, only authorized copies</td>
</tr>
<tr>
<td>TRUSTED BOOT</td>
<td>Detect system software alteration</td>
</tr>
<tr>
<td>AUTHENTICATION WITH TPM</td>
<td>Secure network protocols</td>
</tr>
<tr>
<td>SECURE BOOT</td>
<td>Restrict boot to signed images</td>
</tr>
</tbody>
</table>

APPROTECT: PROTECTION OF THE APPLICATION

The main security threats at the application level are:

- **Integrity**: the running application might be hacked or patched in binary, on the disk or in memory, to modify its behavior or work around some checks.
- **Confidentiality**: the way the application code is working could be analyzed in details by looking at the execution code, in order to learn or to reproduce its behavior.
- **Unauthorized copies**: the embedded systems (software application or full equipment) suffer the risk of being cloned without authorization.

The APPROTECT solution, using a security technology from Wibu, a Kontron partner, protects the application from those risks with the security of a dedicated hardware secure element located on all Kontron boards. All or part of the application execution code is encrypted on the storage device and will only be decrypted in memory in presence of the keys stored inside the secure element. At run time, the integrity of the application in memory is also permanently checked. The application can be fully encrypted as a whole with no modification, or only critical part can be encrypted by using a dedicated API.

Software: Encryption of binary form application is performed in the on-premises Kontron security room by authorized personnel. Purchase of SEC-APPROTECT-INI allows for 10 encryptions for the same project, allowing for software updates. It includes the generation and delivery of the application key for one reference computer.

Hardware: each computer must have the application key in its secure element to be allowed to decrypt and run the software. SEC-APPROTECT-T10 is used to procure keys beyond the first computer.

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:

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-TRUSTEDBOOT-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 password, 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 explicitly prohibited to be booted.

The secure boot service is available on Kontron x86 CPU boards running a UEFI BIOS firmware. Upon delivery of SEC-SECUREBOOT-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 configuration on numerous identical hardware+firmware, SEC-LINE-SECUREBOOT-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

<table>
<thead>
<tr>
<th>ORDER CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEC-Line APPROTECT</strong></td>
<td></td>
</tr>
<tr>
<td>SEC-APPROTECT-INI</td>
<td>Up to 10 application encryptions service over 2 years maximum. Also includes application key generation for one reference computer.</td>
</tr>
<tr>
<td>SEC-APPROTECT-T10</td>
<td>Additional copies of application key for target boards / systems. Qty of 10 over 2 years maximum.</td>
</tr>
<tr>
<td><strong>SEC-Line TRUSTEDBOOT</strong></td>
<td></td>
</tr>
<tr>
<td>SEC-TRUSTEDBOOT-INI</td>
<td>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.</td>
</tr>
<tr>
<td>SEC-TRUSTEDBOOT-T10</td>
<td>Duplication of a reference trusted boot configuration on 10 more identical hardware+firmware+software configuration, over 2 years maximum.</td>
</tr>
<tr>
<td><strong>SEC-Line AUTHENTICATION WITH TPM</strong></td>
<td></td>
</tr>
<tr>
<td>SEC-AUTHENTICATION-INI</td>
<td>Configuration and SSL/TLS certificate for a reference hardware+software configuration to perform authentication with TPM.</td>
</tr>
<tr>
<td>SEC-AUTHENTICATION-C10</td>
<td>Additional SSL/TLS certificates for 10 more identical hardware+software config, over 2 years maximum.</td>
</tr>
<tr>
<td>SEC-AUTHENTICATION-T10</td>
<td>Installation of a reference TPM authentication configuration, including SSL/TLS certificate, on 10 more identical hardware+software, over 2 years maximum.</td>
</tr>
<tr>
<td><strong>SEC-Line SECUREBOOT</strong></td>
<td></td>
</tr>
<tr>
<td>SEC-SECUREBOOT-INI</td>
<td>Configuration and certificates of secure boot for a reference hardware+firmware configuration.</td>
</tr>
<tr>
<td>SEC-SECUREBOOT-K10</td>
<td>Renewal of up to 10 sets of the secure boot keys, due to new software or BIOS change, over 2 years maximum.</td>
</tr>
<tr>
<td>SEC-SECUREBOOT-T10</td>
<td>Duplication of a reference secure boot configuration on up to 10 more identical hardware, over 2 years maximum.</td>
</tr>
<tr>
<td><strong>SEC-Line VULNERABILITY WATCH</strong></td>
<td></td>
</tr>
<tr>
<td>SEC-WATCH-SV</td>
<td>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.</td>
</tr>
</tbody>
</table>

### SUPPORTED PLATFORMS

<table>
<thead>
<tr>
<th>SUPPORTED PLATFORMS</th>
<th>SEC-APPROTECT</th>
<th>SEC-TRUSTEDBOOT</th>
<th>SEC-AUTHENTICATION</th>
<th>SEC-SECUREBOOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>VX305X TPM OPTION</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>VX6090 TPM OPTION</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>VM605X TPM OPTION</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>VX304X TPM OPTION</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>TRACe-X304</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>TRACe-V407</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

## CORPORATE OFFICES

### FRANCE
150 rue Marcelin Berthelot
ZI de Toulon-Est - BP 244
83078 TOULON CEDEX 9
Tel.: + 33 4 98 16 34 00
Fax: + 33 4 98 16 34 01
sales.KFR@kontron.com

### GLOBAL HEADQUARTERS
Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086 0
Fax: + 49 821 4086 111
info@kontron.com

### NORTH AMERICA
9477 Waples Street, Suite 150
San Diego, CA 92121
USA
Tel.: + 1 888 294 4558
Fax: + 1 858 677 0898
info@us.kontron.com

### ASIA PACIFIC
1-2F, 10 Building, No 8 Liangshuihe 2nd Str.,
Economical & Technol. Development Zone,
Beijing, 100176, P.R.China
Tel.: +86 10 63751188
Fax: +86 10 83682438
info@kontron.cn

www.kontron.com