_TrustFence Concept
Atlantik Elektronik GmbH
Digi International Inc.
Agenda

_ATXX Company Structure

_EMBEDDED Device Security

_TrustFence

_ATLANTIK Elektronik Business Unit / Linecard

_Locations
Marketer of semiconductors and IT-products

Semiconductor Division

atlantik elektronik
- Marketer & Design-In specialist of innovative semiconductors
- Marketer of innovative embedded solutions & services

astradis elektronik
- Independent Sourcing

atlantik systeme
- Marketer of network- and communication products and management solutions

IT- Products Division

allmos electronic
- Specialist in Network Analysis and Monitoring
- Marketer of Security Solutions
Embedded Device Security

Security for embedded devices is a critical design aspect

- Security by obscurity is an outdated “concept” - embedded devices are already a high profile target
- IoT already further amplifying existing concerns/issues
- Embedded products require a device security approach supporting their 7-10+ year product lifecycles
- Going beyond secure connections – Access Control, Device Identity/Authentication, Secure Configuration/Deployment/Updates, Encryption, Certificate Management, Secure Boot, Tamper Detection ...

Our Goal: Offer complete, consistent security story for connected embedded devices.
Secure Boot

**What it is**
- Secure Boot is a form of verified booting
- The system firmware checks that the system boot loader is signed with a cryptographic key

**How it works**
- Before handoff to the OS loader, the firmware checks the signature of code
- High Availability Boot (HAB) component of the on-chip ROM enables the ROM to authenticate the program image by using digital signatures.
- This device code will continue the process by ensuring that the peripheral is prepared for handoff to the operating system.
- Signatures are stored in databases in firmware. These databases are the “allowed” and “disallowed” lists that cannot be switched off by software

**Why we need it**
- On the most basic level, Secure Boot prevents running unsigned boot loaders
- Prevents malware to manipulate the boot procedure
- Prevents that malware can bypass OS security features
- Prevents the loading of drivers or OS loaders that are not signed with an acceptable digital signature
Certificate Management

**What it is**
- Creates a comprehensive certificate and key inventory
- Digital certificates are core to implementing a true multi-layered, identity-based security environment.

**How it works**
- Steps: Enrollment, Provisioning, Validation, Monitoring, Notification
- See details about your certificates, modify them, delete them, or request new ones

**Why we need it**
- Certificates and encryption keys protect communications across the Internet
- Making conveniences such as secure online banking, bill paying and shopping possible
- Authenticate identities, verify devices, secure applications and email, and even safeguard website
Secure Storage

**What it is**
- Saves data in an encrypted form
- Uses your operating system account information to provide a single sign-on experience

**How it works**
- Creating a secure encrypted disk
- Your password is passed as data to secure storage.
- Secure storage uses a "master" password to encrypt it and store the encrypted password in a file on disk.
- When data is saved with secure storage, the password provider is selected based on the priorities from the list of enabled password providers. Only that provider can be used in future to decrypt the data.

**Why we need it**
- Protect your data
Secure Ports

What it is
• Management of the TCP/IP Ports of your device

How it works
• Ensure that only the bare minimum of ports are exposed
• Protect open ports, and close the ones that are not used
• Ensure that your firewall is closed to all traffic other than to the ports you know should be open...
• ...and software connected to them is as up to date as possible.

Why we need it
• Hackers are constantly trying to discover new ways to connect to machines
• Whatever their goal, the starting point is the same: the port.
Tamper Proofing

What it is

- Tamper-proofing detects changes in the protected software or its behavior.

How it works

- Encrypted software needs to be decrypted first before an attacker knows what it does.
- Tamper proofing uses lots of encryption but adds an extra element: it hides how the decryption works or what key is used.
- Typically users employ encryption to protect data and tamper-proofing to protect the code.
- Contains elements of checksums and hash codes.

Why we need it

- Tamper-proofing is an active defense against modern attacks.
- Used to hinder, deter or detect unauthorized access to a device or circumvention of a security system.
- Protected against reverse engineering and modification.
Device Identity

What it is
• Specifies unique per-device identifiers
• Distinctive number associated with a specific device

How it works
• Method for authenticating that the device is uniquely bound to that identifier
• Device identification numbers should remain constant for the lifetime of the device

Why we need it
• No standard ways to identify devices across network architectures
• MAC addresses are not sufficient
  • Multiple per device
  • Reconfigurable
  • Not cryptographically bound
• Device identity is important for completing chains of trust
Security Co-Processor

**What it is**
- Dedicated computer on a chip or microprocessor for carrying out cryptographic operations

**How it Works**
- The purpose of a secure crypto processor is to act as the keystone of a security sub-system, eliminating the need to protect the rest of the sub-system with physical security measures.
- Physical attempts to gain access to the internal state of the coprocessor will result in resetting the state of the secure coprocessor

**Why we need it**
- Guarantees the privacy and integrity of the secure system
- Enhances performance and security of cryptographic operations
Secure Connections

**What it is**
- Secure connections are designed to protect data sent between two computers via the Internet

**How it works**
- Data encryption: masking information (emails, for example) from third parties and sender verification
- Encrypting a transfer channel: concealing the entire contents of the network connection and verifying the authenticity of all computers participating in the network connection

**Why we need it**
- Mask confidential data from third parties
- Verify the identification of the party with whom information is being exchanged
- Protect information from being viewed or modified by a third party
TrustFence Concept - Conclusion

System architecture and software platform integration framework

• U-Boot
• Yocto Linux
• Tools
• Documentation

Customer configures level of device security through device personalities

• No implementation effort

Distributed in binary only

• Locked to Digi hardware platforms
• Source code available to customers
Connected and Secure Embedded Communication Platform

- NXP i.MX6UL-2, up to 2 GB NAND (SLC), up to 1 GB DDR3
- Cortex-A7 running at up to 528 MHz (1.9 DMIPS/MHz)
- Cortex-M0+ Microcontroller Assist™ (MKL03Z32CAF4R)
- Integrated very low power and wake-up management assist
- 802.11a/b/g/n/ac 1x1, Bluetooth 4.1, ANT+, Dual Ethernet connectivity
- On-module U.FL antenna connector, or connector-less through pads
- Dedicated on-module security + authentication controller
- UART, USB, SD, CAN, SPI, I2C, I2S, ADC, PWM, GPIO, LCD, camera
- Low-profile, easy-to-use, reliable Digi SMTplus™ surface mount form factor (29x29 mm)
- Industrial operating temperature and long-term availability

**Innovative, cost-efficient, and easy-to-use module solution**

- Secure industrial embedded connectivity platform with long-term availability
- Surface mount module, 29x29mm, allowing automated and manual placement
- Dual-Ethernet and pre-certified dual-band Wi-Fi + Bluetooth 4.1 option using common footprint

**Industrial General Purpose SBC and development board (Pico-ITX)**

- General Purpose SBC with IEC 60068-2 temp/shock/vibe compliance
However beautiful the strategy, you should occasionally look at the results.

*Sir Winston Churchill*
Product Portfolio

**Microcontroller**
- 8 / 16-bit MCU (8051 & proprietary), 32-bit ARM Cortex M0/M3/M4 MCU

**System On Modules - SoM (ARM based)**
- ARM®9 based System on Module w & w/o Wi-Fi & Bluetooth, ARM Cortex A9 ( multicore) based System on Module w & w/o Wi-Fi & Bluetooth

**Single Board Computers - SBC (ARM based)**
- ARM Cortex A9 (multicore) based SBCs w & w/o Wi-Fi & Bluetooth

**Industrial Wi-Fi & Wi-Fi / Bluetooth Combo Frontend Modules**
- USB 2.0 to Wi-Fi / BT Frontend Modules, MiniPCIe to Wi-Fi / BT Frontend Modules, SDIO to Wi-Fi / BT Frontend

**Serial to Ethernet/Wi-Fi Converter (Device Server)**
- Serial to Ethernet, Serial to Wi-Fi, System on Modules

**100/1G/10G Ethernet Products**
- Mag Jacks, Transformer, Jacks, Cables & Plugs

**x86 Peripheral ICs**
- Super I/O controller, Hardware Monitor IC, Power Management IC, Level Shift IC, GPIO Expander, Trusted Platform Module (TPM) solutions
Business Unit Infotainment – A Closer Look

Product Portfolio

**Audio/Video**
- Audio ADC, Audio DAC, Audio Codecs, Audio DSP, Digital Audio Interfaces, Video Encoder/Decoder

**Sensors**
- Magnetic Sensors, Automotive, Current, Infrared, Pressure, Compass

**RF**
- Keyless entry, Mixer, PLL, Two Way Radio

**Displays**
- Passive LCD, Industrial TFT, Automotive TFT, Epaper, Touch panel, Optical optimization
## Product Portfolio

### Bluetooth Smart Ready
- BT Audio and Connectivity ICs and Modules

### Bluetooth Smart
- BT Smart IC/ Modules and Software running on IC/ Module and Apps for Smart Phone

### Wi-Fi
- Wi-Fi ICs and Modules; Wi-Fi/ BT Combos

### Powerline
- Home Plug Green Phy PLC

### Location
- SiRFstarV Multi-GNSS platform and GNSS modules

### DAB & DTV
- Digital Audio & Video Broadcasting, WWR (Radio Chipset & Solution)

### Cellular
- GSM/ GPRS/ UMTS/ HSPA and LTE Modems

### Antenna solutions
Memories – A Closer Look

Product Portfolio

- **SSD NAND Flash Speicher**
  - Industrial SSD, SATA/PATA Flash Module, microSD/SD Cards, CF Cards, USB Flash Module, SATA Flash Module (DOM)

- **Serial Flash** (512 Kb - 512Mb)

- **NAND Flash** (1Gb, 2Gb)

- **Parallel Flash** (32Mb-512 Mb)

- **SDRAM** (16Mb-256Mb)

- **DDR** (64Mb-256Mb)

- **DDR2** (128Mb-2Gb)

- **DDR3** (512Mb-4Gb)

- **Pseudo SRAM** (4Mb-256Mb)

- **Low Power SDR & DDR SDRAM** (1,2V / 1,8V)

- **KGD**

- **2Wire serial EEPROM** (2Kb - 1Mb)
Marketer of semiconductors and IT-products

Locations

Headquarters:
Office Munich
Atlantik Elektronik GmbH
Fraunhoferstraße 11a
82152 Planegg
(Germany)

Offices:

Office Hamburg
Atlantik Elektronik GmbH
Deichstraße 17
20459 Hamburg
Germany

Office Benelux
Atlantik Elektronik GmbH
Mgr. Ariënsstraat 1-02
NL – 5104 KA Dongen
Netherlands

Office Austria
Atlantik Elektronik GmbH
Liebermannstraße A01 303-5
A - 2345 Brunn am Gebirge
Austria

Office Scandinavia
Atlantik Elektronik GmbH
Postboks 58
DK - 2860 Søborg
Denmark

Any Questions?
Dominik Bohn
Field Application Engineer
Telefon: +49 89/89 505-169
mailto:d.bohn@atxx.de
www.atlantikelektronik.com